Carnegie Mellon
Software Engineering Institute

Organizational Models for Computer Security Incident Response Teams (CSIRTs)
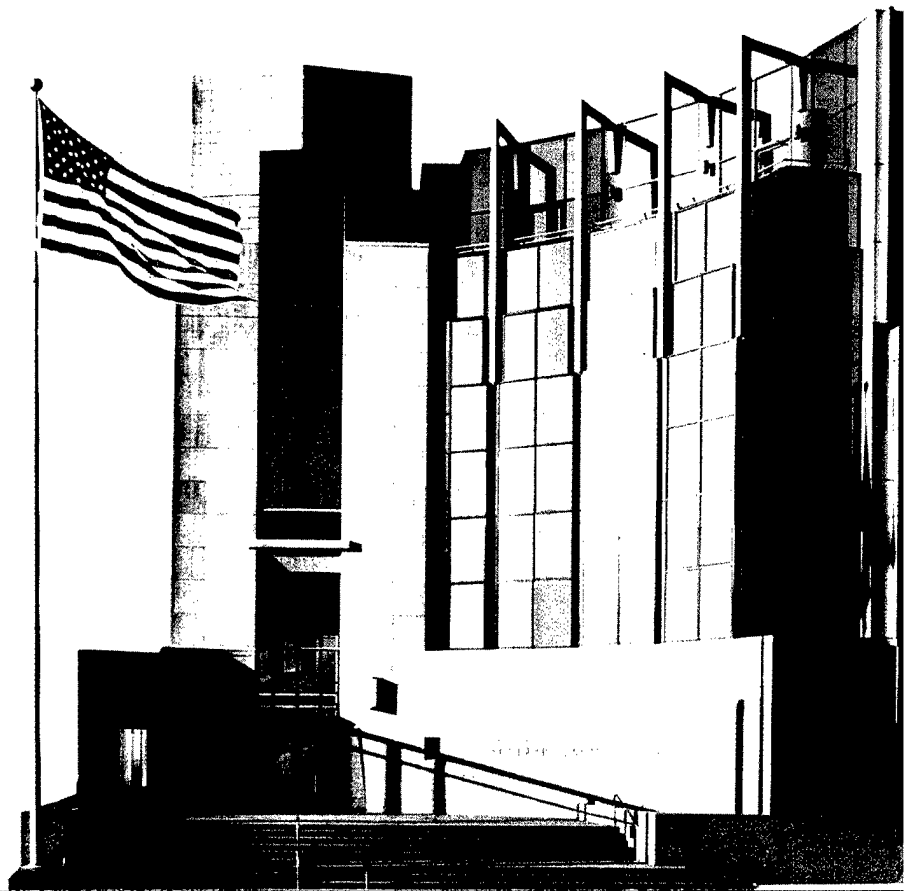
Georgia Killcrece
Klaus-Peter Kossakowski
Robin Ruefle
Mark Zajicek

December 2003

20040412 021

CarnegieMellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Organizational Models for Computer Security Incident Response Teams (CSIRTs)

CMU/SEI-2003-HB-001

Georgia Killcrece
Klaus-Peter Kossakowski
Robin Ruefle
Mark Zajicek

December 2003

Networked Systems Survivability

This report was prepared for the

SEI Joint Program Office
HQ ESC/DIB
5 Eglin Street
Hanscom AFB, MA 01731-2116

The ideas and findings in this report should not be construed as an official DoD position. It is published in the interest of scientific and technical information exchange.

FOR THE COMMANDER

Christos Scondras
Chief of Programs, XPK

Table of Contents

List of Tables

Preface

.

Many organizations today do not provide a formal or focused organizational incident response capability. Computer security and incident response issues are handled by various areas of the organization based on functional and platform expertise. Each area handles and prioritizes security events as they occur on an ad hoc basis. With the increase in the rise of computer security incidents and the decrease in the time organizations have to respond to security events, this uncoordinated approach is no longer sufficient or effective. In light of that, many organizations today are looking to build formalized plans so they are prepared to handle security events when they occur.

Other motivators driving the establishment of formalized computer security incident response team (CSIRT) capabilities today include

- a general increase in the number and type of organizations being affected by computer security incidents

- a more focused awareness by organizations on the need for security policies and practices as part of their overall risk-management strategies

- new laws and regulations that affect how organizations are required to protect information assets

- the realization that systems and network administrators alone cannot protect organizational systems and assets

To help organizations face this situation and create suitable incident response capabilities, *The Handbook for Computer Security Incident Response Teams (CSIRTs)* [West-Brown 98] was written. This publication has become one of the main resources available regarding the formation and management of CSIRTs. This document was revised and updated in 2003 [West-Brown 03]. However, there are still many areas that were not covered in the desired depth by the *Handbook for CSIRTs*, and there were also more areas that could have been explored to some degree. One of these areas, the need for more guidance in the selection of the "right" model for an organization's incident response capabilities, is the topic of this new *Organizational Models for CSIRTs* handbook.

The handbook will focus on the various common organizational structures that a CSIRT might implement, regardless of whether they are from the commercial, educational, government or military sector and regardless of whether they provide an internal service or address

an external constituency consisting of many independent organizations. Some of the issues that will be covered for each different model described in this handbook include

- supported constituencies

- organizational structure

- triage

- available services

- resources

We hope that you will find this companion guide to the *Handbook for CSIRTs* useful in the planning and formation of your CSIRT. You might also find it a useful reference should you need to enhance your already established CSIRT activities. If you think that another organizational structure can better address your organization's needs and requirements, this guide can provide information that may help you determine what model would suit your team and constituency best.

The material in this handbook is based on our experiences in forming and operating our own organization's CSIRTs and through assisting other CSIRTs in their formation and operation. We are always looking to learn from the experiences of other teams. So if you have comments on or suggested additions to this document, or if you want to share your opinions, please contact us. We regularly attend Forum of Incident Response and Security Teams (FIRST) conferences and events,[1] and we can be contacted in person or reached as a group by sending email to the following address: csirt-info@cert.org.

---

[1]   More information on upcoming FIRST conferences can be found at
       <http://www.first.org/events/>.

CMU/SEI-2003-HB-001

Acknowledgements

Abstract

When a computer security attack on an organization occurs, an intrusion is recognized, or some other kind of computer security incident occurs, it is critical for the organization to have a fast and effective means of responding. One method of addressing this need is to establish a formal incident response capability or a Computer Security Incident Response Team (CSIRT). When an incident occurs, the goal of the CSIRT is to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organization.

This handbook describes different organizational models for implementing incident handling capabilities, including each model's advantages and disadvantages and the kinds of incident management services that best fit with it. An earlier SEI publication, the *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002), provided the baselines for establishing incident response capabilities. This new handbook builds on that coverage by enabling organizations to compare and evaluate CSIRT models. Based on this review they can then identify a model for implementation that addresses their needs and requirements.

1 Introduction

When computer security problems occur, it is critical for the affected organization to have a fast and effective means of responding. The speed with which the organization can recognize an incident or attack and then successfully analyze it and respond will dramatically limit the damage done and lower the cost of recovery. Careful analysis of the nature of the attack or incident can lead to the implementation of effective and widespread preventative measures and the avoidance of similar events. This ability to respond quickly and effectively to a computer security threat is a critical element in providing a secure computing environment.

One way to provide such a response is through the establishment of a formal incident response capability. This response capability can be in the form of comprehensive policies and procedures for reporting, analyzing, and responding to computer security incidents. It can also be in the form of an established or designated group that is given the responsibility for handling computer security events. This type of group is generally called a Computer Security Incident Response Team (CSIRT). Focusing a team on incident handling activities allows them to further develop expertise in understanding intruder trends and attacks, along with acquiring knowledge in incident response methodologies. Depending on the services provided, the team can be composed of full-time or part-time staff.

A CSIRT provides a single point of contact for reporting computer security incidents and problems. This enables the team to serve as a repository for incident information, a center for incident analysis, and a coordinator of incident response across an organization. This coordination can extend even outside the organization to include collaboration with other teams, security experts, and law enforcement agencies. The team's relationships with other CSIRTs and security organizations can facilitate sharing of response strategies and provide early alerts to potential problems. As a focal point for incident information, a CSIRT can gather information from across their organization, gaining insight into threats against the constituency that might not have been apparent when looking at individual reports. Based on this information, they can propose strategies to prevent intruder activity from escalating or occurring at all. They also can be a key player in providing risk data and business intelligence to the organization, based on the actual incident data and threat reports received by the CSIRT. This information can then be used in any risk analysis or evaluation.

Having an experienced team established, with defined incident handling procedures in place, can jump start the response process. There is no need to determine who in an organization does what, as there is a team already in place knowing what to look for, who to contact, and

how to affect the response as quickly as possible. CSIRTs located at constituency sites may also have familiarity with the compromised systems and therefore be more readily able to coordinate the recovery and propose mitigation and response strategies.

Depending on its mission and goals, a CSIRT can be structured and organized to provide a range of services in a variety of ways. Of key importance in deciding what types of services to offer will be the type of expertise available and the type of incident handling capability already in place in an organization. Environmental variables, such as organization and constituency size, available funding, and geographic distribution, can also affect the range and level of services provided by a CSIRT. A small, centrally located organization will require a CSIRT that is different from that required by a large, geographically dispersed organization.

Some CSIRTs provide a full set of services, including incident analysis and response, vulnerability[2] handling, intrusion detection, risk assessments, security consulting, and penetration testing. A variety of these full-service teams can be found in the commercial sector. Other CSIRTs provide a smaller set of services. For example, the main service provided by some military organizations is intrusion detection, while some government organizations provide only a referral service, referring incidents to third-party teams. Some teams act as only a central repository to collect reported incident activity. Others act as that central repository and also disseminate any information on new vulnerabilities and intruder trends.

A CSIRT can also be organized as a coordinating CSIRT or coordination center rather than a one-on-one incident response service. In this case, the CSIRT provides information and support to constituent sites at different geographic or organizational locations. These sites can be branches of an organization located in various cities, states, or countries, such as the U.S. Military CSIRTs who coordinate with DOD-CERT,[3] or they can be different independent organizations, such as the member organizations that subscribe to Australian Computer Emergency Response Team (AusCERT) services. These two examples illustrate the different ways that a coordinating CSIRT can work. In the case of DOD-CERT, the team has some authority to enforce some response and mitigation steps across the military. In the case of AusCERT, they have no direct authority over their constituent members but instead provide support, advice, information, alerts, and guidance to those member organizations. In either case, the coordinating CSIRT synthesizes reports and information from all areas to determine the accurate picture of incident activity across the constituency and its vulnerability to attack.

---

[2] A vulnerability is the existence of a flaw or weakness in hardware or software that can be exploited, resulting in a violation of an implicit or explicit security policy.

[3] DOD-CERT is the coordinating CSIRT for the U.S. military.

1.1   Scope of the Document

The purpose of this document is to present a variety of organizational options or models for a CSIRT structure. This report is not designed to be a how-to manual; rather it is a tool to help project managers make informed decisions in the critical early phases of planning their CSIRT capability. This document attempts to illustrate the various issues regarding each option and highlight the decisions that organizations will face when choosing a model.

It should be pointed out that this document only addresses one view of a CSIRT structure, namely, the "organizational" view in regards to the location of the CSIRT staff. There are many other views that can be looked at when determining a CSIRT structure, including how the CSIRT fits into existing business functions and decisions, what sector[4] the CSIRT is part of, or even what mission a CSIRT has. This document does not address these other views, but they are interesting topics for future discussion and publication.

Regarding the decision-making capability and authority of a CSIRT, this document does not discuss how the CSIRT will interact with the business management side of any organization. Depending on the organization and the situation, it is often business factors rather than security factors that will determine what response occurs and at what priority. We do not try to address this at any depth in this document.

Once you have identified a model that best suites your situation, we highly recommend that you follow the guidelines presented in the *Handbook for CSIRTs* [West-Brown 03] to identify the next steps necessary to implement the decision. By being informed and prepared, the management team can focus their energy and resources appropriately and minimize the time and effort associated with building a solid foundation for an effective CSIRT within the organization.

Another document that may be helpful in building or sustaining a CSIRT is *State of the Practice of CSIRTs* [Killcrece 03]. This report provides examples of CSIRT processes, structures, and resources.

1.2   Intended Audience

Like the *Handbook for CSIRTs*, this handbook is a response to observations that many more organizations have recognized the need for a CSIRT. This document is therefore targeted at those who will be most heavily involved in the establishment and strategic direction of CSIRTs, including the decision of which organizational model should be used.

---

[4]   "Sector" in this context means in what business area a CSIRT belongs, such as an educational, government, military, critical infrastructure, or commercial organization.

The primary audience for this document consists of managers who are responsible for the creation of a CSIRT or the creation of an incident handling service. The secondary audience consists of managers who are responsible for the operation of a CSIRT or an incident handling service and who would either like to benchmark their original CSIRT organizational structure against the models or who are looking to potentially reorganize their CSIRT structure and want to understand the considerations and issues involved with each model.

As well as being a useful reference for higher management levels and all CSIRT staff, this document can also be of use to other individuals who interact with CSIRTs and would benefit from an awareness of the issues that affect the organizational setup of any CSIRT. These would include

- members of the CSIRT constituency

- representatives from law enforcement

- representatives from media relations

- representatives from legal counsel

- others parts of the parent organization, including the information technology (IT) department, physical security area, human resources, and any investigative or auditing groups

1.3 Use of this Document

Ideally this document should be used once an organization has obtained management support and approval to form a CSIRT, but prior to the decision of which organizational structure to implement and before the team becomes operational. The document can also be of benefit in the development of any proposals for requesting support, approval, or funding to develop a CSIRT. This material can be used as the basis for understanding the issues involved in selecting a specific organizational structure or configuration for a CSIRT. The information can then be used to assist the development of detailed domain- or organization-specific operational model. This will serve in turn as a foundation to the further development of tailored and detailed service definitions, policies, and procedures.

In addition, members of an existing team can use this document to ensure that they have covered the main issues and options in selecting an organizational structure appropriate for their constituency or team.

It is important to note that this material is provided as a reference or guide for identifying an appropriate organizational model and corresponding services. We do not intend to imply or dictate the range or content of services that any given team should implement. These must be determined on a per-team basis and might even involve combining ideas from the different models presented later in this document to meet a specific team's needs. We encourage you to use the material provided in this document to understand the issues appropriate for your team's

unique environment and decide which approach you should adopt based on your particular goals, needs, and situation.

Chapter 9 of this handbook has been developed as a guide to help you identify what type of CSIRT model may fit your situation. You may want to look at that section before reading about any particular model. Or you may want to read all the model descriptions and see which model best suits your organization.

1.4 Document Structure

The rest of this document is organized as follows:

Chapter 2	**Establishing CSIRT Capabilities**
	Discusses some of the issues that must be addressed when planning a CSIRT or incident management capability. This section also provides some necessary background by explaining different services that might be relevant for any incident handling service and discusses the various ways service offerings can be extended.
Chapter 3	**Organizational Models for CSIRTs**
	Discusses the various organizational structures that can be used to provide incident handling and management services. It also covers the criteria reviewed for each model, including
	• overview of the model
	• supported constituencies
	• organizational structure
	• triage
	• available services
	• CSIRT resources
	• summary of findings
Chapter 4	**Security Team Model**
Chapter 5	**Internal Distributed CSIRT Model**
Chapter 6	**Internal Centralized CSIRT Model**
Chapter 7	**Internal Combined Centralized and Distributed CSIRT Model**
Chapter 8	**Coordinating CSIRT Model**
Chapter 9	**Choosing the Organizational Model for Your CSIRT**
Chapter 10	**Closing Remarks**
Appendix	**Matrix of Models and Corresponding Services**

2 Establishing CSIRT Capabilities

2.1 Overview

There are many issues and questions that must be addressed for any organization to effectively create and implement a CSIRT or any type of incident management capability. High-level management needs to consider the following questions when deciding upon a CSIRT structure and function that best meets the requirements for their organization or constituency.

- What constituency will the CSIRT serve?

- Who is ultimately responsible for security within the organization? The CSIRT will need to have an effective relationship and established communication channels with any group that has anything to do with the security of the enterprise. This should also include interactions with physical security.

- What is the mission of the CSIRT? The basic function and purpose of the CSIRT must be delineated.

- What services will the CSIRT provide? The provision of services is the means by which the CSIRT will fulfill its mission. Will CSIRT staff actually review and repair compromised systems, or will their primary function be to collect, analyze and disseminate information and guidance to others in the constituency?

- What authority will the CSIRT have? This will determine how the CSIRT influences and interacts with the constituency.

- Where will the CSIRT be located, both physically and organizationally? We refer to this as the organizational model for the CSIRT. How is the CSIRT structured and how does it interact with the rest of the constituency?

- What are the roles and responsibilities of the CSIRT staff? What type of expertise is available within the organization or constituency to provide these functions?

- What equipment and network infrastructure is needed to support the daily CSIRT functions?

- How will the CSIRT be funded and sustained?

- How will collaboration occur, and with whom? Established relationships may be needed with legal counsel and law enforcement, public relations, human resources, risk management, crisis management, and infrastructure protection areas of the organization.

- What hours of operation will the CSIRT provide coverage for? Is there a requirement and corresponding funding for a 24x7 operation? If not, what coverage can the organization afford?

While the main focus of this handbook is on the various organizational models for implementing a CSIRT, this cannot be discussed in isolation. Other issues, such as the answers to all of the above questions, are variables that will influence the choice of a model. Most importantly the type of constituency, the chosen mission, and the provided services will play a large role in determining how the CSIRT structure or organizational model will need to be arranged. All of these issues will need to be kept in mind as you review the rest of this document.

2.2 Barriers in Establishing New Teams

Requirements for CSIRTs are just as diverse as the constituents and cultures they serve. Even so, many times organizations look to existing teams for "organizational" examples that might work in their own environments (see the next section). Our experiences in working with other teams and collecting general information on CSIRT structures and practices have helped us identify common team characteristics and practices that may be of assistance to those interested in formalizing a CSIRT capability.

Fundamental differences in mission, goals, and operations make it difficult to define one comprehensive blueprint for creating a CSIRT, although many newly forming teams would be satisfied to have any blueprint at all that could help them in their planning efforts. On the other hand, there are general problems that all new teams will face. For example, we find that

- People who are trained and experienced in incident response techniques and practices are difficult to find.

- No established education path for professional incident handling staff exists as of today. (Much of incident handling activities have been an out-growth of traditional system, network, and security administration.) Most CSIRT education occurs through training and mentoring programs. In recent years certification programs like the CERT-Certified Computer Security Incident Handler[5] and the SANS GIAC Certified Incident Handler (GCIH)[6] have been developed to try to address this need, but where these fit in the overall education path has yet to be determined by many organizations.

- There is a lack of publicly available sample templates for policies and procedures for use in the day-to-day operations of a CSIRT.

- Few tools such as tailored help desk or trouble ticket solutions addressing the specific needs of CSIRTs—authenticity and confidentiality, as well as workflows—are readily available (or at least easily adaptable) to fit into any given CSIRT. However, there are pro-

---

[5] For more information, see <http://www.cert.org/certification/>.
[6] For more information, see <http://www.giac.org/subject_certs.php#GCIH>.

jects in place within the CSIRT community to develop and refine tools that will meet this need. But resources are still needed to complete this type of work.

Without any knowledge about resources that exist, many teams have often had to undergo the same research and learning experience, pulling together the same information that others have already discovered, in an effort to learn how to create and operate their team.

Therefore, we believe that by collecting and providing at least some of the common information about suitable services, organizational structures, and supported constituencies in this handbook, we can make it much easier for the next generation of teams to become established. In turn, they will be able to concentrate on their own internal issues related to this process. As said before, this handbook will concentrate on organizational models. Other follow-on documents will need to be developed to cover other topics of interest to teams that can fill the gaps in the tools, techniques, and training mentioned above.

2.3 Using Existing Teams as Examples

The history of formalized CSIRTs, while only covering 15 years,[7] shows that using existing teams as examples can be one of the best approaches for setting up new teams. In fact, prior to 1998—the year the *Handbook for CSIRTs* became available—no comprehensive document[8] was available for interested organizations to learn about the challenges and tasks associated with establishing a CSIRT.

One of the most beneficial steps a newly forming team can take is to seek opportunities to meet other teams. These can include site visits (your site or theirs), events such as the annual Forum of Incident Response and Security Teams (FIRST)[9] conference, and the regular meetings of regional groups such as the TERENA TF-CSIRT Task Force, a program to promote the collaboration between CSIRTs in Europe[10] or the Asia Pacific Computer Security Emergency Response Team (APCERT), a coordination working group for CSIRTs in the Asia Pacific area.[11] You can also learn about a specific team from information on that team's publicly available web site, if they have one. Many team's web sites have incident reporting forms, guidelines, procedures, and service lists that may provide ideas for your own team. If other teams share common characteristics with your particular situation, such as similar constituen-

---

[7]   As of the date of this publication.

[8]   Certainly there were already papers that highlighted specific issues, but no single document covered the breadth of information related to creating and operating a new team.

[9]   See <http://www.first.org/> for more information regarding the Forum of Incident Response and Security Teams. Past conference programs (as well as conference materials, papers, and presentations since 2000) are available, along with information on upcoming events. The annual conference is generally held in June each year.

[10] See <http://www.terena.nl/tech/task-forces/tf-csirt/> for more information. Past meeting minutes and presentations are available, as well as information on upcoming meetings.

[11] See <http://www.apcert.org/> for more information.

cies or organizational structures, their experience might be especially valuable to your success in planning and implementing your team. However, it is not always the case that a similar team will operate exactly the way your team does. In those cases you may not be able to use the other team's work as a starting point that you can then customize to match your needs.

As mentioned earlier, each CSIRT and the constituency the team serves is different; therefore understanding your constituency and their specific needs is key to determining your CSIRT goals, service offerings, and organizational structure. Any help you can obtain from other teams who went through a similar learning experience will help your plans move forward that much easier. Looking at or visiting similar organizations, identifying their operating characteristics, how they interact with their constituency, and where their CSIRT is located within the organizational structure of the host or parent organization or constituency will be of special interest to you in your planning processes.

Many teams are quite willing to accommodate requests to visit their team and share their experiences (both good and bad) in establishing their own team. They are also generally very supportive in providing resources or information concerning best practices or problem areas they have encountered. In addition, many existing teams consider it important for their day-to-day function to meet other teams, as any future interaction with those teams will facilitate communications, once they have established contact. Such meetings will help teams gain a better understanding of each other and build on an established means of communicating information.

One note of caution, however, is in order: There is no requirement that another team share information or experiences, so do not necessarily expect to receive copies of documents, policies, procedures, or tools. The other team might or might not have such information available, or they might be unable (or unwilling) to share them due to internal policies.

2.4   What's In a Name?

There are many abbreviations that have been used as the basis for team names, as well as characterizing what role the team has. For example,

- IRT = Incident Response Team
- IRC = Incident Response Capability
- IHT = Incident Handling Team
- IMT = Incident Managing / Management Team

Each of the above has been used with other descriptions, such as "Network," "Computer," "Security," "Computer Security," or "Information Technology." So we see as some sample names or titles

- CSIRT = Computer Security Incident Response Team

- CIRT = Computer Incident Response Team

- CIRC = Computer Incident Response Capability or Center

- SIRT = Security Incident Response Team

- SERT = Security Emergency Response Team

In addition, the service marked "CERT" (referring to the CERT® Coordination Center), has been used in combination with other letters[12] by a variety of other teams to characterize their specific team[13] and to build upon a well-established brand name. However, as already mentioned, while the names might be similar, the services offered, the fees, and the levels of support available might be quite different. Similarity in names also does not signify any endorsement or relationship between teams. The variety of names used by teams sometimes makes it difficult for users to understand what a team's position is or how they compare to other teams the user may know about.[14]

It should be noted also that currently[15] there is no "requirement" that exists for naming a team, nor any over-arching authority that "certifies" that a CSIRT is, in fact, a bona fide CSIRT (and accepted as such). In practice, CSIRTs have gained acceptance through the reputation they establish over time and through the trust the team has earned from its constituency and from other external CSIRTs. It should also be noted that some CSIRTs are looking into more formal ways of certification and accreditation as a means of validating or benchmarking the quality of service provided to their constituency. This certification is being discussed for both the team and individual staff level.[16]

As a final note on naming conventions, we should also mention another set of acronyms for service providers, who provide contract "for fee" or membership services. Such contracts (agreements, memoranda of understanding, service level agreements) will detail the services to be provided, as well as the level at which these are offered by the provider. The names generally associated with such providers include but are not limited to

- MSSP = Managed Security Service Providers

- MSP = Managed Service Providers

---

[12]   Use of "CERT" requires permission from the Software Engineering Institute. To obtain permission, send your request to permission@sei.cmu.edu.

[13]   See the FIRST Teams Member List at <http://www.first.org/team-info/> for examples of different CSIRT names.

[14]   To some extent we are similarly guilty, as the terminology we introduce in the rest of this document is not yet well established within the CSIRT community. However, we have selected these conventions because we believe they more precisely describe the roles of the different team models.

[15]   It is certainly possible that in the future some teams will have naming requirements.

[16]   Information about existing certification programs for incident handlers can be found in the CERT *State of the Practice of CSIRTs* report [Killcrece 03].

- ERS = Emergency Response Services

Another acronym is ISAC, which is Information Sharing and Analysis Centers. While MSSP, MSP, and ERS focus on helping individual organizations handle the technical aspects of any incident or attack, ISACs focus on the analytical task at a "sector" level (such as finance, critical infrastructure, telecommunication) to identify trends, risks, and associated mitigation strategies within the sector.

Whatever the naming convention used, it is important that the constituency understands what the CSIRT will (and will not) do in terms of the services it provides. It is also important for any CSIRT to be respectful and understanding of other teams and any services they provide (remembering that each may have different missions, goals, and resources, as we mentioned earlier in this document).

2.5   Defining the CSIRT Constituency[17]

The constituency to be serviced by the CSIRT, including its composition, physical or geographical location or distribution, and the sector in which it is located, will be a deciding factor in choosing an organizational model. A constituency that is composed of one organizational entity such as a commercial business, an educational institution, or a government department will have different organizational needs than a constituency composed of multiple educational institutions who collaborate in a research network or multiple government and critical infrastructure agencies within a country, or multiple national organizations within a region.

Some distinguishing organizational factors that can be used to identify a constituency include

- Internal versus external – Internal means that the CSIRT is in the same organization as the constituency, such as a commercial CSIRT whose constituency is the commercial organization in which the CSIRT is located. So, Siemens commercial organization is the constituency for Siemens CERT. External means the constituency is outside the organizational structure in which the CSIRT is located. For example, the constituency serviced by AusCERT is all the organizations that subscribe to AusCERT services. These organizations are separate legal entities such as commercial businesses, government agencies, and educational institutions. They are all external to the organization in which AusCERT is located.[18] It should be noted that even if a CSIRT services an internal constituency there will still probably be external organizations such as other CSIRTs, law enforcement, and government entities with which they may interact.

---

[17] See the *Handbook for CSIRTs* [West-Brown 03] and the *State of the Practice of CSIRTs* for more detailed information on CSIRT constituencies.

[18] "Internal" and "external" in this context only refers to the relationship the CSIRT has with the constituency. It does not have anything to do with who the CSIRT communicates with.

- Centralized versus distributed – Centralized means the constituency is located close together either physically or geographically, such as being in the same building. Distributed means that the constituency is located across buildings, cities, countries, geographic regions, or even time zones.

2.6 Defining CSIRT Mission

The CSIRT mission[19] should provide a brief, unambiguous description of the basic purpose and function of the CSIRT. This will outline the basic focus of the team, which could include any of the following: recovery of systems, analysis of attacks and intrusions, facilitation and coordination of response activities, coordination of information, investigation of computer crimes, monitoring of intrusion detection systems (IDS). Or it could include some other function specific to the CSIRT.

This mission, together with the CSIRT-provided services, will also influence what type of organizational model is needed. For example, if a team's mission is to actually perform system recovery and patching, then they will need to be able to access the site where the systems are located. If the mission is to only facilitate information exchange and perform analysis to look for trends and patterns in incident activity, then the CSIRT must have mechanisms in place to collect and analyze information from across the constituency. This in turn will require a mechanism for distributing information to the constituency.

2.7 Defining CSIRT Services

Another important issue to be addressed in establishing a CSIRT relates to the range and level of services to be provided to the constituency.

The original version of the *Handbook for CSIRTs* published in 1998 provided a list of common services that a team could provide.[20] In that handbook, the only mandatory service required to be considered a CSIRT was the incident response service. This service definition has been expanded and is now referred to as incident handling,[21] since the work done by a CSIRT is generally more than just "response."

Today the understanding of the services has matured, and the list of possible services that a CSIRT could provide has become larger and more structured. Provision of at least one of the incident handling services—incident analysis, incident response on site, incident response

---

[19] See the *Handbook for CSIRTs* for more information about defining the CSIRT mission.

[20] Originally the list was presented on page 20. Since that time, the *Handbook for CSIRTs* has been updated and now provides a revised and expanded set of services that matches what is presented in this section.

[21] "Incident handling" is used in the *CSIRT Services List* [Killcrece 02].

support, or incident response coordination—is still mandatory to be considered a CSIRT. This new, expanded list of services is outlined in the rest of this section and in the revised edition of the *Handbook for CSIRTs* that was published in 2003. It is also available as a separate web document from the CERT Coordination Center (CERT/CC) web site.[22]

There are a wide variety of services that a CSIRT could choose to offer. Some of the services offered will relate directly to incident handling as a core service of a CSIRT. Other services, such as security training or audits, may only relate indirectly to incident handling, while serving broader organizational security needs. By their very nature, some of the services may also be provided by other parts of an organization, such as IT, training, audits, or some other entity instead of the CSIRT. The actual assignment of tasks and responsibilities will depend on the structure of the parent or host organization in which the CSIRT is located.

Throughout the rest of this handbook we will draw upon this expanded list of services as we discuss which services are suited to which organizational model. For your reference and convenience, the list is included in this section.

A team should not expect to provide every service in the list. It is much better to perform a few services well than many services badly. Also the CSIRT must see where it fits in the constituency's organizational structure. What is provided will be based on what needs the constituency has. It will also be highly influenced by what computer security and incident response related functions are already being performed by existing departments or groups within the constituency.

CSIRT services can be grouped into three broad categories:

- reactive services

  These services are triggered by an event or request, such as a report of a compromised host, wide-spreading malicious code, software vulnerability, or something that was identified by an intrusion detection or logging system. Reactive services are the core component of CSIRT work.

- proactive services

  These services provide assistance and information to help prepare, protect, and secure constituent systems in anticipation of attacks, problems, or events. Performance of these services will directly reduce the number of incidents in the future.

- security quality management services

---

[22] In an effort to consolidate CSIRT service terminology, the Trusted Introducer service for CSIRTs in Europe worked with the CERT CSIRT Development Team in 2002 to produce this updated and more comprehensive list of CSIRT services. It can also be found at <http://www.cert.org/csirts/services.html>.

These services augment existing and well-established services that are independent of incident handling and traditionally performed by other areas of an organization such as the IT, audit, or training departments. If the CSIRT performs or assists with these services, the CSIRT's point of view and expertise can provide insight to help improve the overall security of the organization and identify risks, threats, and system weaknesses. These services are generally proactive but contribute indirectly to reducing the number of incidents.

The services are listed in Table 1 and described in detail below.

Table 1:   CSIRT Services by Category

Reactive Services	Proactive Services	Security Quality Management Services
✦ Alerts and Warnings	○ Announcements	✓ Risk Analysis

✦ Incident Handling
  – Incident analysis
  – Incident response on site
  – Incident response support
  – Incident response coordination
	○ Technology Watch
	○ Security Audit or Assessments
	○ Configuration & Maintenance of Security Tools, Applications, & Infrastructures
		✓ Business Continuity & Disaster Recovery Planning
		✓ Security Consulting
		✓ Awareness Building
		✓ Education/Training

✦ Vulnerability Handling
  – Vulnerability analysis
  – Vulnerability response
  – Vulnerability response coordination
	○ Development of Security Tools
	○ Intrusion Detection Services
		✓ Product Evaluation or Certification

✦ Artifact Handling
  – Artifact analysis
  – Artifact response
  – Artifact response coordination
	○ Security-Related Information Dissemination	

Note that some services have both a reactive and proactive side. For example, vulnerability handling can be done in response to the discovery of a software vulnerability that is being actively exploited. But it can also be done proactively by reviewing and testing code to determine where vulnerabilities exist, so the problems can be fixed before they are widely known or exploited.

2.7.1 Reactive Services

Reactive services are designed to respond to requests for assistance, reports of incidents from the CSIRT constituency, and any threats or attacks against CSIRT systems. Some services may be initiated by third-party notification or by viewing monitoring or IDS logs and alerts.

Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus, or hoax, and providing any short-term recommended course of-action for dealing with the resulting problem. The alert, warning, or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected. Information may be created by the CSIRT or may be redistributed from vendors, other CSIRTs or security experts, or other parts of the constituency.

Incident Handling

Incident handling involves receiving, triaging,[23] and responding to requests and reports, and analyzing incidents and events. Particular response activities can include

- taking action to protect systems and networks affected or threatened by intruder activity

- providing solutions and mitigation strategies from relevant advisories or alerts

- looking for intruder activity on other parts of the network

- filtering network traffic

- rebuilding systems

- patching or repairing systems

- developing other response or workaround strategies

Since incident handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Incident analysis. There are many levels of incident analysis and many sub-services. Essentially, incident analysis is an examination of all available information and supporting evidence or artifacts related to an incident or event. This may include analysis of network, host, and application audit logs; intruder toolkits, malicious code, and any other supporting information. The purpose of the analysis is to identify the scope of the incident, the extent of damage caused by the incident, the nature of the incident, and available response strategies or workarounds. The CSIRT may use the results of vulnerability and artifact analysis (described below) to understand and provide the most complete and up-to-date analysis of what has happened on a specific system. The CSIRT correlates activity across incidents to determine any interrelations, trends, patterns, or intruder signatures. Two sub-services that may be done as part of incident analysis, depending on the mission, goals, and processes of the CSIRT, are

---

[23] Triaging refers to the sorting, categorizing, and prioritizing of incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital, where patients who need to be seen immediately are separated from those who can wait for assistance.

- **forensic evidence collection**: the collection, preservation, documentation, and analysis of evidence from a compromised computer system to determine changes to the system and to assist in the reconstruction of events leading to the compromise. This gathering of information and evidence must be done in a way that documents a provable chain of custody that is admissible in a court of law under the rules of evidence. Tasks involved in forensic evidence collection include (but are not limited to) making a bit-image copy of the affected system's hard drive; checking for changes to the system such as new programs, files, services, and users; looking at running processes and open ports; and checking for Trojan horse programs and toolkits. CSIRT staff performing this function may also have to be prepared to act as expert witnesses in court proceedings. This service can also include conducting personnel interviews to determine what took place.

- **tracking or tracing**: the tracing of the origins of an intruder or identifying systems to which the intruder had access. This activity might involve tracking or tracing how the intruder entered the affected systems and related networks, which systems were used to gain that access, where the attack originated, and what other systems and networks were used as part of the attack. It might also involve trying to determine the identity of the intruder. This work might be done alone but usually involves working with law enforcement personnel, Internet service providers (ISPs), or other involved organizations.

Incident response[24] on site. The CSIRT provides direct, on-site assistance to help constituents recover from an incident. The CSIRT itself physically analyzes the affected systems and conducts the repair and recovery of the systems, instead of only providing incident response support by telephone or email (see below). This service involves all actions taken on a local level that are necessary if an incident is suspected or occurs. If the CSIRT is not located at the affected site, team members would travel to the site and perform the response. In other cases a local team may already be on site, providing incident response as part of its routine work. This is especially true if incident handling is provided as part of the normal job function of system, network, or security administrators in lieu of an established CSIRT.

Incident response support. The CSIRT assists and guides the victim(s) of the attack in recovering from an incident via phone, email, fax, or documentation. This can involve technical assistance in the interpretation of data collected, providing contact information, or relaying guidance on mitigation and recovery strategies. It does not involve direct, on-site incident response actions as described above. The CSIRT instead provides guidance remotely so site personnel can perform the recovery themselves.

Incident response coordination. The CSIRT coordinates the response effort among parties involved in the incident. This usually includes the victim of the attack, other sites involved in the attack, and any sites requiring assistance in the analysis of the attack. It may also include

---

[24] Note that "incident response" is used here to describe one type of CSIRT service. When used in team names such as "Incident Response Team," the term typically has the broader meaning of incident handling.

the parties that provide IT support to the victim, such as Internet service providers, other CSIRTs, and system and network administrators at the site. The coordination work may involve collecting contact information, notifying sites of their potential involvement (as victim or source of an attack), collecting statistics about the number of sites involved, and facilitating information exchange and analysis. Part of the coordination work may involve notification and collaboration with an organization's legal counsel, human resources, or public relations departments. It would also include coordination with law enforcement. This service does not involve direct, on-site incident response.

Vulnerability Handling

Vulnerability handling involves receiving information and reports about hardware and software vulnerabilities, analyzing the nature, mechanics, and effects of the vulnerabilities, and developing response strategies for detecting and repairing the vulnerabilities. Since vulnerability handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Vulnerability analysis. The CSIRT performs technical analysis and examination of vulnerabilities in hardware or software. This includes the verification of suspected vulnerabilities and the technical examination of the hardware or software vulnerability to determine where it is located and how it can be exploited. The analysis may include reviewing source code, using a debugger to determine where the vulnerability occurs, or trying to reproduce the problem on a test system.

Vulnerability response. This service involves determining the appropriate response to mitigate or repair a vulnerability. This may involve developing or researching patches, fixes, and workarounds. It also involves notifying others of the mitigation strategy, possibly by creating and distributing advisories or alerts.[25] This service can include performing the response by installing patches, fixes, or workarounds.

Vulnerability response coordination. The CSIRT notifies the various parts of the enterprise or constituency about the vulnerability and shares information about how to fix or mitigate the vulnerability. The CSIRT verifies that the vulnerability response strategy has been successfully implemented. This service can involve communicating with vendors, other CSIRTs, technical experts, constituent members, and the individuals or groups who initially discovered or reported the vulnerability. Activities include facilitating the analysis of a vulnerability or vulnerability report; coordinating the release schedules of corresponding documents, patches, or workarounds; and synthesizing technical analysis done by different parties. This service can also include maintaining a public or private archive or knowledgebase of vulnerability information and corresponding response strategies.

---

[25] Other CSIRTs might further redistribute these original advisories or alerts as part of their services.

Artifact Handling

An artifact is any file or object found on a system that might be involved in probing or attacking systems and networks or that is being used to defeat security measures. Artifacts can include but are not limited to computer viruses, Trojan horse programs, worms, exploit scripts, and toolkits.

Artifact handling involves receiving information about and copies of artifacts that are used in intruder attacks, reconnaissance, and other unauthorized or disruptive activities. Once received, the artifact is reviewed. This includes analyzing the nature, mechanics, version, and use of the artifacts; and developing (or suggesting) response strategies for detecting, removing, and defending against these artifacts. Since artifact handling activities are implemented in various ways by different types of CSIRTs, this service is further categorized based on the type of activities performed and the type of assistance given as follows:

Artifact analysis. The CSIRT performs a technical examination and analysis of any artifact found on a system. The analysis done might include identifying the file type and structure of the artifact, comparing a new artifact against existing artifacts or other versions of the same artifact to see similarities and differences, or reverse engineering or disassembling code to determine the purpose and function of the artifact.

Artifact response. This service involves determining the appropriate actions to detect and remove artifacts from a system, as well as actions to prevent artifacts from being installed. This may involve creating signatures that can be added to antivirus software or IDS. The main focus of this function is artifact remediation.

Artifact response coordination. This service involves sharing and synthesizing analysis results and response strategies pertaining to an artifact with other researchers, CSIRTs, vendors, and security experts. Activities include notifying others and synthesizing technical analysis from a variety of sources. Activities can also include maintaining a public or constituent archive of known artifacts and their impact and corresponding response strategies. The main focus of this function is the gathering and sharing of artifact intelligence.

2.7.2 Proactive Services

Proactive services are designed to improve the infrastructure and security processes of the constituency before an incident or event occurs or is detected. The main goals are to avoid incidents and to reduce their impact and scope when they do occur.

Announcements

This includes, but is not limited to, intrusion alerts, vulnerability warnings, and security advisories. Such announcements inform constituents about new developments with medium- to

long-term impact, such as newly found vulnerabilities or intruder tools. Announcements enable constituents to protect their systems and networks against newly found problems before they can be exploited.

Technology Watch

The CSIRT monitors and observes new technical developments, intruder activities, and related trends to help identify future threats. Topics reviewed can be expanded to include legal and legislative rulings, social or political threats, and emerging technologies. This service involves reading security mailing lists, security web sites, and current news and journal articles in the fields of science, technology, politics, and government to extract information relevant to the security of the constituent systems and networks. This can include communicating with other parties that are authorities in these fields to ensure that the best and most accurate information or interpretation is obtained. The outcome of this service might be some type of announcement, guidelines, or recommendations focused at more medium- to long-term security issues. This service becomes almost an intelligence-gathering function. Coupled with lessons learned from live data, this can be a powerful service to provide.

Security Audits or Assessments

This service provides a detailed review and analysis of an organization's security infrastructure, based on the requirements defined by the organization or by other industry standards[26] that apply. It can also involve a review of the organizational security practices. There are many different types of audits or assessments that can be provided, including

- infrastructure review—manually reviewing the hardware and software configurations, routers, firewalls, servers, and desktop devices to ensure that they match the organizational or industry best practice security policies and standard configurations

- best practice review—interviewing employees and system and network administrators to determine if their security practices match the defined organizational security policy or some specific industry standards

- scanning—using vulnerability or virus scanners to determine which systems and networks are vulnerable

- penetration testing—testing the security of a site by purposefully attacking its systems and networks. Penetration testing can include social and physical attacks as well as network attacks. Checking on the physical security of critical data and servers and testing whether key staff can be easily social engineered into performing unwanted actions or giving away

---

[26] Industry standards and methodologies might include: Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), CCTA Risk Analysis and Management Method (CRAMM), Information Security Forum's Fundamental Information Risk Management (FIRM), Commonly Accepted Security Practices and Regulations (CASPR), Control Objectives for Information and (Related) Technology (COBIT), Methode d' Evaluation de la Vulnerabilite Residuelle des Systemes d'Informa (MELISA), ISO 13335, ISO 17799, or ISO 15408.

confidential information is just as important as testing whether network attacks can make it through the existing perimeter and internal defenses.

Obtaining upper management approval is required before conducting such audits or assessments. Some of these approaches may be prohibited by organizational policy. Some approaches may also have legal or regulator implications that must be taken into account. Activities crossing any kind of border, whether country, state, provincial, or some other geographic designation, may be subject to an entirely different set of laws. On the other hand, there may be strict legal compliance requirements that the CSIRT and parent organization need to meet, and these should be built into the audit or assessment criteria.

Providing this service can include developing a common set of practices against which the tests or assessments are conducted, along with developing a required skill set or certification requirements for staff that perform the testing, assessments, audits, or reviews. This service could also be outsourced to a third party contractor or managed security service provider with the appropriate expertise in conducting audits and assessments.

Configuration and Maintenance of Security Tools, Applications, Infrastructures, and Services

This service identifies or provides appropriate guidance on how to securely configure and maintain tools, applications, and the general computing infrastructure used by the CSIRT constituency or the CSIRT itself. Besides providing guidance, the CSIRT may perform configuration updates and maintenance of security tools and services, such as IDS, network scanning or monitoring systems, filters, wrappers, firewalls, virtual private networks (VPN), or authentication mechanisms. The CSIRT may even provide these services as part of their main function. The CSIRT may also configure and maintain servers, desktops, laptops, personal digital assistants (PDAs), and other wireless devices according to security guidelines. This service includes escalating to management any issues or problems with configurations or the use of tools and applications that the CSIRT believes might leave a system vulnerable to attack.

Development of Security Tools

This service includes the development of any new, constituent-specific tools that are required or desired by the constituency or by the CSIRT itself. This can include, for example, developing security patches for customized software used by the constituency or secured software distributions that can be used to rebuild compromised hosts. It can also include developing tools or scripts that extend the functionality of existing security tools, such as a new plug-in for a vulnerability or network scanner, scripts that facilitate the use of encryption technology, or automated patch distribution mechanisms.

Intrusion Detection Services

CSIRTs that perform this service review existing IDS logs, analyze and initiate a response for any events that meet their defined threshold, or forward any alerts according to a predefined

service level agreement or escalation strategy. Intrusion detection and analysis of the associated security logs can be a daunting task—not only in determining where to locate the sensors in the environment, but collecting and then analyzing the large amounts of data captured. In many cases, specialized tools or expertise is required to synthesize and interpret the information to identify false alarms, attacks, or network events and to implement strategies to eliminate or minimize such events. Some organizations choose to outsource this activity to others who have more expertise in performing these services, such as managed security service providers.

Security-Related Information Dissemination

This service provides constituents with a comprehensive and easy-to-find collection of useful information that aids in improving security. Such information might include

- reporting guidelines and contact information for the CSIRT
- archives of alerts, warnings, and other announcements
- documentation about current best practices
- general computer security guidance
- policies, procedures, and checklists
- patch development and distribution information
- vendor links
- current statistics and trends in incident reporting
- other information that can improve overall security practices

This information can be developed and published by the CSIRT or by another part of the organization (IT, human resources, or media relations), and can include information from external resources such as other CSIRTs, vendors, and security experts.

2.7.3 Security Quality Management Services

Services that fall into this category are not unique to incident handling or CSIRTs in particular. They are well-known, established services designed to improve the overall security of an organization. By leveraging the experiences gained in providing the reactive and proactive services described above, a CSIRT can bring unique perspectives to these quality management services that might not otherwise be available. These services are designed to incorporate feedback and lessons learned based on knowledge gained by responding to incidents, vulnerabilities, and attacks. Feeding such experiences into the established traditional services (described below) as part of a security quality management process can improve the long-term security efforts in an organization.

Depending on organizational structures and responsibilities, a CSIRT may provide these services or participate as part of a larger organizational team effort.

·The following descriptions explain how CSIRT expertise can benefit each of these security quality management services.

Risk Analysis

CSIRTs may be able to add value to risk analysis and assessments. This can improve the organization's ability to assess real threats, provide realistic qualitative and quantitative assessments of the risks to information assets, and evaluate protection and response strategies. CSIRTs performing this service would conduct or assist with information security risk analysis activities for new systems and business processes or evaluate threats and attacks against constituent assets and systems.

Business Continuity and Disaster Recovery Planning

Based on past occurrences and future predictions of emerging incident or security trends, more and more incidents have the potential to result in serious degradation of business operations. Therefore, planning efforts should consider CSIRT experience and recommendations in determining how best to respond to such incidents to ensure the continuity of business operations. CSIRTs performing this service are involved in business continuity and disaster recovery planning for events related to computer security threats and attacks.

Security Consulting

CSIRTs can be used to provide advice and guidance on the best security practices to implement for constituents' business operations. A CSIRT providing this service is involved in preparing recommendations or identifying requirements for purchasing, installing, or securing new systems, network devices, software applications, or enterprise-wide business processes. This service includes providing guidance and assistance in developing organizational or constituency security policies. It can also involve providing testimony or advice to legislative or other government bodies.

Awareness Building

CSIRTs may be able to identify where constituents require more information and guidance to better conform to accepted security practices and organizational security policies. Increasing the general security awareness of the constituent population not only improves their understanding of security issues but also helps them perform their day-to-day operations in a more secure manner. This can reduce the occurrence of successful attacks and increase the probability that constituents will detect and report attacks, thereby decreasing recovery times and eliminating or minimizing losses.

CSIRTs performing this service seek opportunities to increase security awareness through developing articles, posters, newsletters, web sites, or other informational resources that explain

security best practices and provide advice on precautions to take. Activities may also include scheduling meetings and seminars to keep constituents up to date with ongoing security procedures and potential threats to organizational systems.

This awareness building may also include reports and briefings for management, to not only discuss the "state of the organization" in regards to computer security issues but also to educate management on the implications and effects of taking or not taking various security actions and precautions. This education will also include helping management understand security problems and mitigation strategies.

Education/Training

This service involves providing information to constituents about computer security issues through seminars, workshops, courses, and tutorials. Topics might include incident reporting guidelines, appropriate response methods, incident response tools, incident prevention methods, and other information necessary to protect, detect, report, and respond to computer security incidents. This service could also include training on specific types of incidents or vulnerabilities, as well as educating constituents about social engineering, SPAM, viruses, and virus hoaxes.

Product Evaluation or Certification

For this service, the CSIRT may conduct product evaluations on tools, applications, or other services to ensure the security of the products and their conformance to acceptable CSIRT or organizational security practices. Tools and applications reviewed can be open source or commercial products. This service can be provided as an evaluation or through a certification program, depending on the standards that are applied by the organization or by the CSIRT.

2.7.4   CSIRT Core Services

It is recommended that any team that wants to be considered a CSIRT start with a suitable subset of services that it can realistically support with existing resources and staff, gain the acceptance of the organization by providing those services in a quality manner, and then develop any further capabilities as other services are needed and can be effectively supported.

Although we mentioned that a CSIRT needs to provide (at a minimum) an incident handling service, in reality, most teams we see forming today provide much more. As a result, a baseline set of services has emerged that appears to be appropriate for initial consideration by any CSIRT.

This baseline set of services has been developed from resources such as the *Handbook for CSIRTs*, the collective knowledge and experience in incident response activities gained over the last decade by CERT/CC and many other teams, discussions with other CSIRTs, a review

of available literature, and a pilot organizational survey of CSIRTs done as part of the research for the *State of the Practice of CSIRTs* report.

The base list of services is the services we commonly found being offered across CSIRTs. We are not saying that every CSIRT must provide these services; we are saying that we found in most teams that one or more of the following services were being offered. Therefore, for a team starting out, they may find that this list gives them an idea of what types of services they may want to consider. It is essential that the advertised set of services for a CSIRT be achievable with the available resources and skills, so deciding which set of services to initially offer must be done with care. As mentioned before it is better to offer a few services well than many services badly. A CSIRT that is thought to perform badly will find it very difficult and time-consuming to repair a negative opinion about their operations and their usefulness to their constituency. Poor performance and the resulting damage to the reputation, integrity, and trustworthiness of the CSIRT are often irreparable.

The baseline set of services consists of the following:

- Reactive Services
    - alerts and warnings
    - incident handling
        - incident analysis
        - and *at least one* of the following: incident response on site, incident response support, incident response coordination
    - vulnerability handling
        - vulnerability response coordination[27]
- Proactive Services
    - announcements
- Security Quality Management Services
    - awareness building
    - security consulting—specifically security policy development

The core set of services offered by any team will be specific to their situation. Teams can offer any number of services in whatever combination they choose or are required to provide, but experience shows us that it is very difficult to claim to be a CSIRT and to not at least provide

---

[27] It is important to note that this only refers to accepting information about vulnerabilities and passing that information along to another group or team for further investigation, response, analysis, and other support. It is a very basic handling of the information to facilitate dissemination to the appropriate individuals.

some form of the above reactive services related to the incident handling functions (incident analysis, response support, response on site, or response coordination).

2.7.5 Extending Service Offerings

Over time, there will inevitably be changes in the environment of any CSIRT, whether this is due to changes in funding, the staff working in the team, technology, or other external influences. In the same way, there are situations where changes will be actively pursued by the CSIRT itself to adjust its services and service levels, or more likely to extend its service offerings to address a newly recognized need.

Such service needs can be related to

- changes in the constituency that might require different services and/or service support (for example, a need is identified for routine security evaluations by the CSIRT to ensure that efficient baseline security measures are applied by constituent members)

- new organizations or departments that are integrated into the constituency and that now request on-site support by CSIRT staff members instead of support by telephone or by email, as was previously provided

- the CSIRT offering its services (as a whole or in terms of a customized service package) to a completely different constituency

It is also the case that a more market-oriented point of view can be taken. For example, from a business perspective, a CSIRT already providing services may see an opportunity to generate additional revenue by offering similar services to other subscribers or customers. Or an existing team may find that the activity within its constituency has changed and a new service is warranted. This could also be a situation where business considerations call for changes. A commercial CSIRT might expand its service availability to 24 hours a day, 7 days a week, 365 days a year instead of providing service for standard local business hours only.

Strategic considerations might also influence selection of services, e.g., striving for a specific market position nationally or internationally. As a final example, a commercial CSIRT seeking to be recognized for specializing in a type of service, such as automated security audits, might heavily market that capability.

These situations can be similar to some of the decisions you will face before actually building your CSIRT. You will need to assess the conditions, requirements, and options available and choose those services that best fit your situation.

In addition to how changes evolve to address business considerations, there are also a few "natural progressions" that have been observed in the evolution of a variety of CSIRT services. Remember as you read these, however, that some services may have no or very small econo-

mies of scale. This must be considered as you decide if you will expand your service offerings. For example, to take on services such as forensics analysis will require more staff, more time, more tools, and more training than may be available and these skills might not end up being used frequently. Meanwhile developing an advisory service may reach a broader audience with not as much investment.[28]

2.7.5.1 Building New Services on Existing Services

Many of the services mentioned throughout this handbook have similar requirements with regard to the necessary information, experience, and skills needed to provide a specific service. Understanding the interconnections between different services will greatly help to extend the range of services over time. The chances for the success of new services that build on existing services are higher, and the costs of ramping up such services can be lower.

Furthermore, the implied (or suggested) evolution of service offerings in the sections described below can also illustrate the benefits of providing services with close interconnections. Not only do the services benefit from each other in this evolution, but the same staff members involved with one service might also provide the other service(s) as well. But a word of caution must be made here: before adding or expanding services, you need to be sure that funding and staffing levels are appropriate. Staff cannot take on additional services without expanded funding and resources. Managers must be careful to avoid staff burnout and overstretching staff commitments. Staff must be available to handle incidents as they occur, and large-scale major events can require dedicated time and staff.

It is also important to note that changes in services might also mean that a change in organizational model is needed to adequately provide the new services. For example, a team might evolve from a local security team to a centralized or coordinating CSIRT.

Note: The arrow in the following titles implies that a CSIRT delivering the service on the left of the arrow can evolve into the service on the right of the arrow under the conditions discussed in each section. Also, these services could only evolve if there was adequate time available for the CSIRT to provide the new service and, of course, only with management approval.

Awareness Building ➔ Education/Training

To be successful, training must build on the achievement of general security awareness by the constituent population. Deficiencies in awareness can be identified through feedback received

---

[28] Certainly there are and will continue be other migration paths besides CSIRT services that can change the focus of a team (from traditional incident handling services to a more research or analysis-related work, or coordination capability); but they are not covered here. These other services will, of course, also be dependent on the knowledge and expertise readily available within or obtainable by the CSIRT.

during training courses or as the result of constituency behavior that allows various computer security incidents to occur.

Since awareness building utilizes some of the approaches and mechanisms that are also used in education and training, a team providing awareness building has already established the foundation for more elaborate training sessions and an education program. All it needs is to formalize the coverage and the technical depth of the material. Some of the necessary infrastructure might already be available within other parts of the organization (e.g., IT, human resources, or a corporate training department).

Security Consulting ➔ Risk Analysis / Business Continuity

While security consulting in the general sense might deal with questions related to risk analysis or business continuity, at a CSIRT level it is much more likely that it relates specifically to some dedicated problem areas (remote access) or more practical security problems (firewall or host system configuration). Security consulting by a CSIRT can be provided based on the specific expertise available in the team, but the full-fledged risk analysis/business continuity planning and assessment, which addresses all technologies and applications used in the constituency, needs to build on a much more elaborate knowledgebase and practice as each of these areas have their own methodologies and frameworks. Risk analysis and business continuity planning (or disaster recovery planning) is usually done by specialists with skills and backgrounds in those areas.

For a CSIRT, the evolution to such a service may be much longer to achieve and may need to be carefully orchestrated, as staff will need to acquire these new skill sets and also to avoid unnecessary duplication of effort with whoever is currently performing these services in the organization. One way to migrate into providing such a service is to work collaboratively with those in the organization who have this background and skill set. The CSIRT, with its involvement in incident data collection, can provide authenticated risk data to the risk management process. They can also provide input into the security configurations most suited to the organization. In this way they can begin to work as part of the team that does provide the risk analysis and business continuity planning service. If no one in the organization is already providing these services, then the work done by the CSIRT can begin to fill this gap.

Vulnerability / Artifact Analysis and Response ➔ Security Audit and Assessments
Vulnerability / Artifact Analysis and Response ➔ Intrusion Detection

The knowledge gained from analyzing artifacts and vulnerabilities is important for providing robust security audits and assessments, as well as maintaining up-to-date intrusion detection configurations. In many cases, both services are looking at similar issues from different perspectives: Security audits look for new vulnerabilities and attacks that can compromise the security of systems from an *attacker's* point of view; intrusion detection does the same but from the *defender's* point of view.

Previously gained knowledge from the Vulnerability as well as Artifact Analysis and Response activities provides a natural progression for team members with this expertise to contribute to security audit and assessment initiatives and intrusion detection activities. It should be pointed out, however, that performing security audits and assessments requires a specific skill set and application of definitive techniques. CSIRT staff will probably not transition into these positions but rather provide information to the security audit and assessment functions, providing criteria and requirements in the security area that need to be reviewed and evaluated.

Vulnerability Analysis and Response ➜ Vulnerability Response Coordination

The coordination of efforts related to any response to new vulnerabilities requires an extensive knowledge of vulnerability analysis and response. The CSIRT must understand the situations that vendors face when a new vulnerability is identified in one of their products and have a long-term, trusted relationship with the vendor community.

Once a team undertakes vulnerability analysis and response, cooperation with vendors, other CSIRTs, organizational system, network, and security administrators, and other security experts will inevitably lead to a situation where such interactions need to be coordinated.

Product Evaluation ➜ Configuration and Maintenance of Security Tools/ Applications/Infrastructure ➜ Development of Security Tools

The relationships between these three services are also dependent on the common knowledge and background for each.

Just the evaluation of specific products or of products belonging to a specific group of tools by itself will provide the constituency with useful information. Some of the knowledge gained .through such product evaluations can serve to kick-start an extension of the service to the configuration and the maintenance of a specific product (one that is selected based on the evaluation).

The progression to the next level of service, and the development of new tools, generally has one of two goals:

1. to solve weaknesses in existing products that should be mitigated

2. to address gaps that should be closed and missing functionality that should be addressed

These goals build on knowledge gained through extensive experience with existing tools and products. Staff involved in delivering these services also require a background in secure programming practices and system architectures.

In summary, the above sections describing how services might evolve over time has been included as an illustration of ways in which CSIRTs might modify and extend their services as a

team matures. As your new team is developing a strategy and becomes operational it might also be useful to consider how the team's services could potentially evolve over time. Such considerations in the early phases of your development and planning discussions will help to identify the infrastructure, tools, staff, and skill set that will be needed in the future to ensure that your CSIRT operations continue to effectively serve your constituency.

2.7.5.2 Building New Constituencies on Existing Services

Throughout this document we stress that the focus of any CSIRT service needs to be tailored towards the needs of the constituency, whether it be an organization or a group of many separate organizations. But it is also true that, once the CSIRT service is fixed for any constituency, other constituencies could be identified that have similar needs. Another progression in the evolution of a CSIRT could be that it provides a set of well-defined services to a different set of customers (or a completely new constituency).

There are some examples, such as the dCERT[29] service offering, where a previously internal team started to provide a commercial service, taking advantage of their expertise and the established infrastructure. A key factor in dCERT's successful transition was the personnel or staff of the organization. Because the team members had experience based on their internal work, they were able to successfully transition to a wider commercial audience. It is important to note that in this example the commercial service created uses clearly outlined contracts that detail the service offerings and service levels associated with them.

It would be much more difficult to position a team from a commercial organization as the "national" team (for a region, country, etc.), since many of the stakeholders (constituents) involved could fear a conflict of interest. The situation might be viewed differently if the team is serving a large constituency and has already established a not-for-profit or neutral position.[30]

Any political issues need to be addressed before any migration towards new constituencies should be planned. From a team's business perspective it can certainly be advantageous to expand their scope of service delivery.

- Higher return of investments may be realized as more customers are served (without necessarily increasing internal resources proportionately).

- An improved reputation could attract more customers or other sources of funding (which could lead to even more expanded or new services being introduced).

---

[29] dCERT started as internal CSIRT team within DaimlerBenz, later DaimlerChrysler, and is now a commercial service offering from T-Systems ISS GmbH, Germany. See <http://www.dcert.de/> for more information.

[30] Such evolutions (from a commercial team to a national team) are theoretically possible, but we are not aware of any real-life examples.

- Improved insight into the overall status regarding incidents, computer crimes, and victims involved will in turn provide an opportunity to create informed statistics and assessments that may not otherwise be available.

On the other hand, there are some arguments, against using the same team to serve different constituencies. Foremost is the potential conflict of interest—for example, even multinational organizations like Siemens prefer to have a clearly defined, internal team that is separate from the team that handles product vulnerabilities. This is done to avoid any possibility of such a conflict of interest. This is most significant when a CSIRT is providing for-fee services to external customers. In such a case, if there are two incidents, one involving internal systems, the other from an external customer, it is better that they are handled by separate teams. If an incident involved not only the systems of an external customer but also an internal system, the external customer might question the neutrality of the CSIRT feeling that they may favor or protect the internal customer over the external customer. More than that, such a situation could present a legal conundrum with respect to negligence and disclosure.

The key factor for any CSIRT that considers adding new constituencies to its already existing base constituency (this is also true for any service changes) is that the team must fulfill all requirements for and provide suitable interfaces with any supported constituencies. This requires careful planning and may also require additional resources. The CSIRT must also look at its existing organizational model and determine if that structure will adequately support the new additional constituency. If not, then a different model may be appropriate and may need to be implemented.

3 Operational Issues

3.1 Overview

Along with the issues discussed in Chapter 2, there are many operational issues that will need to be addressed or considered when establishing a CSIRT capability. The primary focus of this document is the organizational model or operational structure of the team. This involves the physical location of the team, the place of the team in the parent organization or constituency, and how the CSIRT interacts with the rest of the constituency. It can also involve who the CSIRT reports to in the organization, the authority of the CSIRT within the constituency, and the way information flows into and out of the CSIRT.

3.2 Common Organizational Models for CSIRTs

In Chapters 4 through 8 of this document, five generic organizational models for a CSIRT are presented. These models are briefly described below.

- **Security Team:**[31] In this model, no group or section of the organization has been given the formal responsibility for all incident handling activities. No CSIRT has been established.

  Available personnel, usually system, network or security administrators, at the local or division level handle security events on an ad hoc and sometimes isolated basis as part of their overall responsibilities or job assignments. Incident response efforts are not necessarily coordinated or standardized across the organization. There may be no group or designated individuals available to gather information across the organization to scope the damage or impact of incident activities, analyze trends, report to senior management, or provide either effective recovery or protective steps. This is a "business as usual" approach and provides only very limited and unpredictable reactive incident handling capabilities.

- **Internal Distributed CSIRT:** In this model, the organization utilizes existing staff to provide a "virtual" distributed CSIRT, which is formally chartered to deal with incident response activities.

---

[31] Within the context of this handbook, the reference to security team is used in a generic sense. We acknowledge that some organizations have clearly defined groups of expert staff who are assigned to a more formalized Security Team, a team that has very specific roles and responsibilities, but not within the ad hoc context used in this description.

There is a manager who oversees and coordinates activities for the distributed team. Across the organization, individuals are identified as the appropriate points of contact for working as part of the distributed team based on their expertise with various operating-system platforms, technologies, and applications; or based on their geographic location or functional responsibilities. The distributed team members can perform CSIRT duties in addition to their regular responsibilities or could be assigned to CSIRT work on a full-time basis.

The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

- **Internal Centralized CSIRT:** This model is a fully staffed, dedicated CSIRT that provides the incident handling services for an organization.

  In many cases team members spend 100% of their time working for the CSIRT; however, this type of model could also be provided using part-time staff on a rotation basis. There is a CSIRT manager who reports to high-level management such as a chief information officer (CIO), chief security officer (CSO), or even chief risk officer (CRO) or some other equivalent manager. The team is centrally located in the organization and is responsible for all incident handling activities across the constituency or enterprise.

  The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

- **Internal Combined Distributed and Centralized CSIRT:** This model represents a combination of the distributed CSIRT and the centralized CSIRT. It maximizes the utilization of existing staff in strategic locations throughout the organization with the centrally located coordinating capabilities of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency within the enterprise.

  The CSIRT serves as the single point of contact into the organization in relation to incident or vulnerability reports or activity for both internal and external parties.

- **Coordinating CSIRT:** In this model the CSIRT coordinates and facilitates the handling of incidents across a variety of external or internal organizations, which could include other CSIRTs. The CSIRT can be a coordinating entity for individual subsidiaries of a corporation, multiple branches of a military organization, institutions in a research network or specific domain, or for various organizations within a particular country or state. Coordinating CSIRTs usually have a broader scope and a more diverse constituency.

  What makes this model unique is the set of services provided and how they are tailored towards helping other organizations deal with incident handling issues. Very often coordinating CSIRTs have no authority over the members of their constituency. Their main function is to provide incident and vulnerability analysis, support, and coordination services. They can distribute guidelines, advice, warnings, and recommended mitigation and recovery solutions.

Some organizations may find that they actually fall between two models or that their organization comprises multiple levels of CSIRT-related functions and actually encompass more than one model.

3.3 Other Issues

As previously mentioned there are other operational issues besides the organizational model that must be taken into account when establishing CSIRT capabilities. These factors will also influence the required organizational model and will affect the success level of any CSIRT.

3.3.1 Triage

Triage is the process of sorting, categorizing, and prioritizing incoming incident reports or other CSIRT requests. It can be compared to triage in a hospital where patients who need to be seen immediately are separated from those who can wait for assistance.

Triage is an essential element of any CSIRT. It is on the critical path for understanding what is being reported throughout the organization. It serves as the vehicle by which all information flows into the CSIRT. Triage allows for an initial assessment of an incoming report and queues it for further handling. The triage function provides an immediate snapshot of the current status of all activity reported to the CSIRT—what reports are open or closed, what actions are pending, and how many of each type of report has been received. Triage provides an overview of activity being reported to the CSIRT. This process can help to identify potential security problems and help to prioritize the CSIRT workload. Information gathered during triage can also be used to generate trend information and statistics for upper management.

The triage process is important for providing an understanding of the scope of the reported incident activity. Depending on how the organization is physically and geographically structured, triage can be provided various ways:

- If the constituency is distributed in nature, each geographic area, division, or department can provide a help desk or incident response hotline to receive requests from that area (this may also include a special email alias for receiving email requests). In this method, the team members at the distributed site do the initial triage of the requests and reports. They also ensure that all requests are forwarded to a central tracking database so that all reports can be synthesized, correlated, and analyzed.

- Another method of providing this function might be to have all incident reports come into the CSIRT, itself. In this approach, the CSIRT receives all incident and vulnerability reports directly. There is a specific CSIRT email alias, phone number, or web form for reporting incident activity. The CSIRT has its own hotline or help desk for the enterprise, staffed with members from the team. This staff receives, categorizes, and initially priori-

tizes all phone, email, and web reports and requests. Incident reports or vulnerability reports are passed on to appropriate CSIRT analysts for handling.

- A third method could be to have triage performed separately from the CSIRT. In this structure, the CSIRT works very closely with an enterprise-wide help desk. Help desk personnel serve as the funnel through which all information flows, but they are not part of the CSIRT. As the focal point for the initial collection, sorting, assignment, and tracking of reports, the help desk takes requests by phone, email, or web form. For the help desk to be successful in this activity the constituency must be given clearly defined guidelines for reporting and the help desk staff must be well trained to recognize and pass on security issues and problems to the CSIRT. The help desk staff also need to fully understand any information disclosure policies and must be able to be trusted to handle sensitive information properly.

  For this triage model to work correctly, help desk personnel need to understand the services provided by the CSIRT and need to know when to seek assistance from CSIRT members. The CSIRT must be able to work closely with the help desk staff to review or reassign trouble reports to the appropriate individuals in the CSIRT for follow-up. The CSIRT will also require access to the help desk database. CSIRT staff (along with help desk personnel) need to be able to review trouble reports, modify those reports with updated information, open new reports, reassign reports, and close or reopen reports. Any information that is deemed confidential or sensitive may need to be stored in a different database or archived with access restricted to CSIRT staff. A secure communications mechanism between these two entities will also be needed.

Whatever approach is used, it is important to have widely distributed guidelines for reporting incident activity to the CSIRT. These guidelines should be available to all staff via an internal web site or similar function. It is important that the constituency clearly understand the organization's security policies and procedures; all users must understand the importance of reporting attacks, viruses, and any other suspicious or abnormal activity to the CSIRT. There must be no fear of retribution or repercussions for reporting activity. The key to success here is to establish an environment where individuals want to report suspicious activity. If they have a fear of reporting because of a perceived negative effect they will not report to the CSIRT. Some teams have implemented anonymous reporting to specifically address these types of concerns.

Because the centralized reporting and triage processes provide a way to coordinate the collection of information, it is possible to know what type of activity is being observed or reported across the organization. The CSIRT can therefore identify in a more efficient and timely manner whether critical system and network services are being attacked and act accordingly.

When creating and implementing a CSIRT, the method by which triage will occur will need to fit the operational and organizational needs of the constituency. This will be another decision to be made as a part of the implementation process.

3.3.2 Authority

Authority describes the control that the CSIRT has over its own actions and the actions of its constituents related to computer security and incident handling activities. Authority is the basic relationship the CSIRT has to the organization it serves.

According to the *Handbook for CSIRTs*, there are three distinct levels of authority that a CSIRT can have with its constituency: full, shared, and none.

1. **Full authority:** If a CSIRT has full authority, it can direct the constituency to perform the actions or response steps necessary to enhance the organization's security posture or to recover from an incident. During a security event, if warranted, the CSIRT can make the decision to take action without waiting for approval from higher level management. For example, with full authority a CSIRT can tell system administrators to disconnect systems from the network during an attack, or can isolate the systems themselves.

2. **Shared authority:** If the CSIRT has shared authority, it works with the constituency to influence the decision-making process concerning what actions should be taken. The CSIRT can influence the outcome of the decision, but it is a participant in the decision-making process, rather than the decision maker. In this case the CSIRT can recommend that systems be disconnected from the network during an attack and discuss actions to be taken (or repercussions if recommendations are not followed) with the rest of the constituency.

3. **No authority:** If a CSIRT has no authority, it can only act as an advisor to the organization (*albeit* a very strong advisor). The CSIRT cannot make any decisions or take any actions on its own. The CSIRT can recommend that systems be disconnected during an attack but it would not have a vote in the final decision. However, its role can be to raise the security implications that would result if its recommendations are not followed. The CSIRT may be able, because of its position and reputation in the organization, to influence the decision makers to act for the overall good of the organization.

Another type of authority highlighted in the *Handbook for CSIRTs* is "indirect authority." In this case, the CSIRT due to its position may be able to exert pressure on the constituent to take a specific action. An ISP for example may be able to strongly encourage its constituents to take a specific action or face discontinuation of Internet services.

The *Handbook for CSIRTs* also mentions some services that might not be possible if the CSIRT has no authority over its constituency.[32] Although the topic of authority is not considered in detail for the various models described here, such potential conflicts are highlighted. Some model descriptions do include a brief discussion of the suggested authority required for the model to work effectively.

---

[32] For a detailed discussion of this topic, refer to the *Handbook for CSIRTs*, Section 2.1.2.3, Relationship to Constituency.

For a CSIRT to be successful in its mission, it is critical that management approves and supports the level of authority that the team will have. Otherwise, the team will lose credibility in the organization and will not be successful. Management should also adequately and clearly convey the CSIRT authority to the constituency—particularly division managers, system and network administrators, and any other groups within the organization (e.g., IT departments, public relations, legal counsel, other management staff) that would be affected by any decisions made by the CSIRT.

Please note that in regards to the decision-making capability and authority of a CSIRT, this document does not describe how the CSIRT will interact with the business management side of any organization. Depending on the organization and the situation, it is often business factors, not security factors, that determine what response occurs and at what priority. We do not address this at any depth in this document. But anyone planning a CSIRT will need to take this issue into consideration.

3.3.3 Existing Teams in an Organization

In addition to issues related to identifying the best place for the CSIRT within the organization (its organizational position and reporting relationships), the existence of any other team(s) or group(s) already involved and performing incident handling tasks will need to be addressed to avoid any conflicts and to ensure that the constituency clearly understands the roles and responsibilities of each group.

If, for example, a different team in the organization is already handling computer virus incidents, then it is essential to consider this team or group and how it will interrelate to any new CSIRT team established in the organization. Options could include the virus-handling functions being absorbed by the new CSIRT or the virus-handling team, itself, becoming part of the CSIRT. Another option might be to keep the virus-handling team as a separate entity and have the CSIRT concentrate on other types of security problems and intruder activity. This last option would still require coordination between the two groups to ensure that all relevant activity is reported to the right team.

Whatever option is chosen, policies, processes, and procedures will need to be established that detail how these two teams will work together, including what information is shared between the two, what type of assistance each can provide to the other, and what type of notification (if any) occurs between the two concerning any ongoing incident event or activity.

Experience shows that if care is not taken to develop the correct synergy, conflicts may (and often do) occur that will affect future relationships, not only between the existing teams/groups, but also with the constituency that is being served. This can negatively impact any CSIRT. It is very important to get the support and buy-in from any other teams or groups involved in handling incidents or computer security issues to ensure the success of any CSIRT.

Consider another example in which teams, each handling separate services, are now coordinated under a centralized CSIRT (e.g., an existing security team, a virus protection team, and maybe a separate team that handles network security monitoring). Not only should the services of the newly forming CSIRT be considered and determined based on already-available services, but the notion of the CSIRT as a single point of contact for the organization as a whole must be evaluated to determine if it could affect already-established cooperation and communication links to other teams or vendors. Care must be taken to avoid detrimentally affecting such existing relationships. It will be vital to the overall success of the CSIRT to ensure that important communication links within the community are not broken. It is important to adopt solutions that allow for the necessary centralized reporting and coordination, while preventing any bottleneck or interruption of existing working relationships.

One suggested approach in the above example could be to extend the services offered by the existing team or group instead of creating an entirely new component within an organization. In some situations, such an option has some inherent advantages. The issues related to these migrations are discussed in more detail in Section 2.7.5.

3.4   Comparison of Organizational Models

So that readers can effectively compare the CSIRT organizational models presented in the following chapters, we have described each in a similar manner. In this section we explain the topics addressed for each model:

- Overview
- Supported Constituencies
- Organizational Structure
- Triage
- Available Services
- CSIRT Resources
- Summary

These topics in essence become the criteria by which each model can be compared and through which recommendations can be made.

3.4.1 Overview

The overview provides a general description and introduction to the model.

3.4.2 Supported Constituencies

Not every organizational model will support every type of potential constituency in the best and most effective way. More specifically, not all services of a particular organizational model will address the most urgent needs of any possible constituency.

Besides choosing the right services (see Section 2.7), knowing the limitations in supporting particular constituencies will help to prevent some common pitfalls.

In this section, we discuss the constituencies most suitably supported by a given model.

3.4.3 Organizational Structure

This section describes the CSIRT's place in the organization—that is, its organizational position and reporting relationships. It may also describe the physical and geographic location of the team. In addition, communications, both internal and external, are discussed here.

3.4.4 Triage

This section of each model will discuss any specific triage processes that might be required by or affect the structure of a particular organizational model.

3.4.5 Available Services

As described earlier in this document, a CSIRT can offer a wide variety of services based on its mission and purpose. The "Available Services" section of each model discusses how such services will be delivered (or possibly not delivered) under the model. This section also provides the rationale for why services work best in a particular model. This section is broken down into core services that the CSIRT can provide in the model and additional services that might be provided. Core services are those that are best suited to the model and that are the main focus of the CSIRT.

In reading each section the reader may see services commonly described across the various models. This occurs because even though the model is different, the service is still provided in a similar manner.

3.4.6 CSIRT Resources

This section will include any special considerations or requirements regarding staffing, equipment, and infrastructure that are required to support the model. For additional detailed discussion of these resources, refer to the *Handbook for CSIRTs*.

3.4.7 Summary

This section will highlight the effect the model has on the organization's constituency and will also detail the strengths and weaknesses of the models.

The remainder of this document will describe each of the organizational models in more detail in separate chapters. Chapter 9 provides a brief guide to help readers determine what type of model their constituencies might need, if they are not sure which model to consider. These chapters are followed by a closing remarks summary section.

3.4.8 Appendix

The appendix contains a matrix showing the different CSIRT models and the corresponding core and additional services that are provided as part of each model.

4 Security Team—Using Existing IT Staff

4.1 Overview

The security team model is not a typical CSIRT model. Rather, it is the exact opposite: it is the absence of a formal CSIRT. In this model, there is no centralized functional area or group that is given the overall responsibility for providing or coordinating an incident handling capability. Incident handling tasks and services are conducted by the system and network administrators or other security experts who normally maintain, configure, and protect the organization's hosts and networks.

These system, network, and security administrators are loosely called the security team because their job functions involve internal and external security defenses. For example, they handle security issues and technologies such as firewalls, antivirus filters, secure remote access, and intrusion detection.

The term "security team" can refer to individuals who perform these functions or to a group of individuals who work as a team. These individuals might be located in a centralized site, but more often are distributed across the enterprise.

In this model there is really no cross-organizational authority for providing incident response, collecting and analyzing incident data, or implementing recovery and mitigation steps. Instead, teams or individuals are locally responsible for security in their part of the organization. All authority for implementing any security policies and response efforts falls to the departments, divisions, or functional business units. Each of these areas has full internal authority for determining when an incident has occurred within their department or business unit and for deciding what recovery steps to take. Authority may, in fact, rest with non-technical managers working in conjunction with their system, network, or security administrators.

Typically with this kind of model, little coordination of incident information and response occurs, since each area performs tasks on an as-needed basis. It is a minimalist or "business as usual" model, in which no extraordinary measures are taken to prepare a coordinated response to security events by the organization as a whole. The members of the security team deal with incidents in an ad hoc approach as part of their day-to-day work. This model is very reactive and is not conducive to the provision of proactive services.

The goals of the security team are generally to protect systems and networks, detect abnormalities, and if necessary respond to the abnormalities that are identified. Their basic mission is to return the affected systems to operational status as soon as possible. To provide more than these services, an organization probably needs to choose one of the other models discussed later in this document.

We would be remiss if we did not acknowledge that there are indeed instances where the security team model is implemented and works effectively in performing both reactive and proactive incident handling tasks. Usually this is due to the fact that the staff involved go beyond their normal responsibilities to ensure information is coordinated. It can also result when enterprise-wide policies and procedures are enforced regarding incident reporting and incident response and when specific notification and information sharing policies are in place. The security team, although not a formal CSIRT, in many respects performs its role as such. In that regard they are considered a pseudo internal distributed team for all intents and purposes.

4.2 Supported Constituencies

The security team model is often found in organizations that have a narrow, focused need for security-related administration. As this need is recognized, small teams may be established to handle particular security issues or areas that require even more specialization. Most often, organizations start with dedicated teams for central security infrastructure components like firewalls, virtual private networks (VPNs), intrusion detection systems (IDS), remote access points, or antivirus scanning and prevention. Other work can include maintenance and implementation of security configurations for host systems. By virtue of doing this type of work, the members of these teams handle any other security issues that may occur.

These teams may consist of multiple staff or just one individual. Collectively, these specialized teams make up what is called the security team in this handbook.

This model is usually found in a commercial business, government department, or educational institution.

4.3 Organizational Structure

There is no real organizational structure for incident management in this model. The focus for incident reporting is division and platform based because that is where the hardware and software expertise lies. Responsibility for security and incident issues rests with the system, network, or security administrators. These administrators are scattered throughout the enterprise and do not usually have a centralized means of communication or collaboration for incident

handling efforts.[33] Each division and its operational staff end up being the policy- and decision-making entity rather than just the implementer of response efforts. However, the divisions still support and follow any enterprise-wide security or IT policies.

There is generally no centralized repository of incident data that can be used by the organization to generate an overall picture of incident activity, unless one can be provided through an organizational help desk.

There is also generally no one assigned with specific incident handling experience to work with external groups, the media, law enforcement, or other CSIRTs. Usually these tasks fall to the existing organizational public relations coordinator and legal counsel. Because there are no designated incident handling liaisons, any member of the security team might call for assistance from other security experts, other CSIRTs, other coordination centers, or law enforcement. This can often be done in isolation, with the requesting party not realizing that another part of the organization is already in touch with the third party experts. In turn it can make it confusing for the third party, as they are talking to many different people in the same organization.

4.4   Triage

Triage[34] in this model is handled in an ad hoc manner, as no single reporting point has been identified. Each part of the security team will evolve its own reporting and triage mechanisms based on the policies of the division or department in which it is located. Contact points where incidents may end up being reported might include the general help desk; a specific divisional help desk; designated system, network, or security administrators; or the informal office "gurus."

Under this model, each part of the security team may develop its own set of procedures for processing, sorting, and prioritizing incoming information. There may be no formal record keeping; or if there is, there most likely is no way to consolidate the information that is obtained unless, as mentioned previously, a centralized help desk is being utilized. In such an environment, it is difficult or impossible to know what type of activity is being observed or reported across the enterprise, because there is no comprehensive mechanism for reporting, sorting, and disseminating information. Even if information is collected it may not necessarily be what is needed to coordinate an effective response.

---

[33]   Although there can be, for example, email notification lists that are set up to share information, we have often seen that such notification still does not ensure or invoke a coordinated response.

[34]   Even in the absence of a formal method, triage implicitly occurs when system and network administrators scan their incoming mail for information and tasks that need to be handled and determine what additional steps need to be taken.

Without a coordinated effort, categorization and analysis of information can be handled differently across the enterprise, resulting in inconsistent or even incorrect incident evaluation, prioritization, or response.[35] Without a mandate to report information to a centralized point, no true picture of incident activity can be synthesized for the enterprise. In a structure such as this, to gain a high-level view of the enterprise, someone must be designated as the central point for collecting incident information and activity. If this type of synthesis of incident activity is to be done, the key questions will be where is this central point located in the enterprise and what staff will be assigned this responsibility? In most cases, for centralized reporting and analysis to work, one of the other models discussed in this handbook is needed.

4.5 Available Services

The following sections describe those CSIRT services that might be provided in a security team model. It is recognized that every organization is different, so these are general descriptions based on observations of and discussions with organizations using a security team model. The method in which the service is delivered assumes a certain level of infrastructure, staff, and equipment, which is discussed later.

4.5.1 Core Services

Because most often in the security team model there is no centralized or coordinated group for providing incident management and because the operational goal of organizations with this type of model is to recover and repair damaged systems and networks, the following services are those generally offered. The emphasis on repairing systems makes the security team's main function focus on incident response. Note that they are somewhat different from the normal core services offered by CSIRTs that are discussed in Section 2.7.4.[36]

Incident Analysis

Incident analysis in this model is usually done only at the surface level to determine what has happened and what mitigation steps are necessary to get affected systems operational. Any deeper analysis such as incident correlation or trend analysis will most probably not be done, as the security team will focus on reacting to the computer security event, rather than proactively working to prevent future occurrences.

Initial incident analysis is done on a divisional or departmental basis or by the available members of the security team. Even the person reporting an event might do the analysis. The analysis will be focused on determining if a security incident has occurred, how widespread the ac-

---

[35] This is not to say that a security team model cannot have an integrated tracking and reporting system. But our experience shows that normally this is one of the weaknesses of this type of model.

[36] Again, your individual experiences or requirements may differ.

tivity is at the local level, and what impact it is expected to have. The analysis can also include researching existing information and strategies to help mitigate the activity.

Problems that can result using a security team model involve duplication of effort, lack of consistent analysis processes, and sometimes lack of expertise on the part of the security team staff on how to effectively respond to incident events.

Depending on the staff member's level of expertise, they may or may not be able to identify that a problem exists, or how severe it is. They may only be able to identify a symptom (not the real cause of the problem), and may or may not know who to call. Those who are sufficiently knowledgeable and can perform the analysis may not share their results with others, instead focusing only on building a response strategy for their own local systems.

Different members of the security team may conduct very different types of analysis, since there is no standard methodology. Duplicate effort will very likely be expended by other divisions or locations in addressing similar types of incidents and reports. Without sharing this information, the amount of time it takes to resolve an incident across the enterprise increases, effectively resulting in a more costly recovery process. Problems that could have been prevented will instead spread across the enterprise, causing more down time, loss of productivity, and damage to the infrastructure. If information is indeed shared, the recipients may not be sufficiently skilled to implement the repairs in an effective manner.

As mentioned previously, incorrect conclusions can be drawn and insufficient actions taken to address similar problems, depending on the expertise of the administrator or individual investigating the activity. Some areas will respond quickly because they understand what has occurred and know what needs to be done to repair the damage. Others might need to seek advice, guidance, or approval, which could delay analysis and response. Still others might misdiagnose the problem and apply inadequate solutions that do not completely address the problem—or worse, introduce even more serious vulnerabilities. Without consolidating the collected information, there is no mechanism for identifying security trends, patterns, or potential problems that can affect the entire organization.[37] Activity might go unreported or unnoticed because no notification of what to look for was disseminated.

Incident Response On Site

As with triage and incident analysis, incident response is handled at the local level. Response efforts are most likely left to system, network, and security administrators. This service fits well within the security team model as the members of the team are located throughout the enterprise so they are located where the activity will need to be addressed. They will also, due

---

[37]   There are some security teams we have seen that work together and follow established incident response procedures. In most cases this is due to the dedication, commitment, and expertise of the personnel involved. If these personnel leave for some reason, the process often collapses.

to their other work responsibilities, have experience with the systems and networks in their purview, which can help in the resolution of incident activity. The response work will be done as an extension of their normal duties.

However, just because members of the security team are familiar with the systems and networks and are strategically located, does not mean that they will have the expertise to handle an incident and resolve it correctly. This is a major down side of the security team model, that staff are not necessarily trained in correct incident response processes or methodologies. They may also not be familiar with various intruder attacks and corresponding mitigation strategies. These administrators may not realize the potential seriousness of an event, might fail to give the response the appropriate priority, or not know to whom to elevate more serious threats. Reports can be handled more than once because the origin or source of the problem is not addressed, only the symptom. Since there is no formal mechanism for sharing information or lessons learned as a result of handling a particular type of event, potential knowledge relating to this activity may be lost.

Also because members of the security team do incident response and also perform other duties, this can potentially cause a conflict in prioritizing their workload. If other work takes precedence and incidents are not recognized or addressed in a timely fashion, then activity can cause further damage or erroneous responses to reports. Each report very likely is handled anew, resulting in the organization unnecessarily expending additional resources. The next time a similar report is received, it may even be sent to a different group of security experts within the organization.

With this limited localized response, it is unlikely that there is any significant sharing of information with other parts of the enterprise, let alone externally with other CSIRTs.

If critical system and network services are attacked, only local system, network, or security administrators who are directly involved with those systems or services are aware of the activity, and they may or may not be able to repair the damage. For example, if there is a virus outbreak in another part of the organization, only the people who work with systems in that area may be aware that there is a problem. They may fix the problem without letting personnel in any of the other areas know what has occurred. Other parts of the enterprise can suffer from the same virus and have to solve the same problem again, without the ability to leverage the benefit of work already done. In addition, solving the same problem multiple times across other parts of the enterprise will incur additional costs, result in loss of time and effort that could have been devoted to other tasks, and can even result in different (possibly incorrect) solutions being applied.

Incident Response Coordination

Incident response coordination in this model is performed at a minimal level, usually only within the affected division or group. Extended coordination may be required if the response

actions that need to be taken are under the control of a different department; for example, if filters need to be installed on the enterprise firewall but the administrators handling the incident do not have control of the firewall. In this case a channel must be established to ask the appropriate people to make the changes to the firewalls. Often in the security team model these formal channels do not exist, so it may be difficult to not only find who to talk to about having the changes made, but also difficult to have the appropriate people comply in a timely manner.

With incident response handled individually in each area and without the benefit of a centralized reporting area, there is also no way to create standard responses that can be used across the organization. Another problem resulting from this structure is that there is no way to ensure that systems, patches, and virus updates are made in a consistent manner or that they are even made at all across the enterprise. Each division can only be responsible for ensuring that their administrators have complied with the recommended mitigation strategies.

Since response work is done at the local level, there is no point of contact to handle any requests or questions from external sources or to pass on information to external sources. Information about external sites and organizations involved in the incident might (or might not) be passed to other relevant CSIRTs to allow them to contact these organizations directly. It is unlikely that there is consistent or complete reporting to all external parties, especially if an incident involves a large number of sites. The security team members generally do not have the resources to contact many sites nor possibly the tools and skills to facilitate such coordination even if they want to take the appropriate steps to contact and inform others.

The success of any coordination effort in this model depends on how well various team members work together. It also depends on having clear procedures for notification of other parts of the constituency or enterprise, and a clear means of escalation of incident activity if necessary. Along with procedures, a list of the members of the security team and their contact information is needed, so that the appropriate people within the constituency can be notified.

Vulnerability and Artifact Response

As part of their normal security tasks, members of a security team undertake actions to mitigate or repair a vulnerability, as well as to determine the appropriate actions to detect and remove artifacts such as viruses, Trojan horse programs, toolkits, and exploits from a system.

In addition, the members of the security team determine what other protective measures need to be taken to avoid future similar or equivalent attacks and incidents. This usually involves researching and applying patches, fixes, and workarounds. It may involve creating signatures that can be added to virus scanning databases or intrusion detection systems.

If members of the security team are scattered across a constituency or organization, they may not readily share analysis of exploits or problems they have discovered or mitigation strategies resulting from their testing and research. This can cause inconsistent remediation efforts to be applied throughout the enterprise.

Configuration and Maintenance of Security Tools, Applications, and Infrastructures

This generally is the main service provided by the members of the security team. This is their normal day-to-day work: maintaining the availability and security of the local environment and infrastructure.

The system and network components configured and maintained can include firewalls, VPNs, IDS, or even virus scanners. Work may also involve user account and password management or the review of network, system, security, and accounting logs.

Depending on how security standards have been implemented in the parent or host organization, this configuration and maintenance may be done along enterprise-wide guidelines or by divisional guidelines. Unfortunately, if it is done divisionally, this may mean that different areas of the enterprise are not protected as effectively as others, and therefore could be more vulnerable.

If the security policies are divisionally based, and different security settings are used across the enterprise, then this may also affect how efficiently and timely response efforts can be applied throughout the parent or host organization. If other parts of the enterprise do not use the same security policies, tools, or configurations, then more work will be needed to determine what comparative action can be taken.

Intrusion Detection Services

This service can be provided in one of two ways: either centrally by one department or unit in the enterprise, or divisionally. If it is handled divisionally, multiple efforts are expended to review the IDS logs and determine what actions to take. Also, there is usually no consolidation of information across the enterprise to provide a "big picture" of intrusion activity for use in the analysis of trends and patterns.

4.5.2 Additional Services

In addition to its core services, a security team may facilitate other services. The following services are those most likely to be provided.

Alerts and Warnings

Because it is the mission of security teams to handle security configuration and maintenance tasks for their parts of the organization, they are the appropriate point of contact to receive alerts and warnings sent from other security-related organizations or vendors. They can use this information to determine prevention and mitigation strategies to handle vulnerabilities, intruder attacks, or other related computer security problems. They may also be given the responsibility to disseminate the information to others within the organization or constituency. Besides alerts and warnings forwarded from others, they may disseminate annotated messages and alerts and warnings they have composed. In all, their tasks may include collecting, evaluating, distributing, and perhaps even developing alerts and warnings. However, this depends on their having enough time to do this work. Often the normal day-to-day work may keep the staff so busy that they cannot send out alerts in a consistent manner. It is possible that alerts may be sent out only on an occasional or emergency basis.

If the security team has no designated authority, any alerts they send out may be ignored by other groups unless management requires that the alerts be followed.

Vulnerability and Artifact Analysis[38]

In the context of a security team, any work in regard to the analysis of vulnerabilities or artifacts is initiated by a real need, most often by an incident or attack detected by the security team. If there is no standard methodology to follow, the analysis done is usually ad hoc and inconsistent. The analysis is also limited to the technical expertise of the available local analysts and most probably focused on a particular event.

If there are no resources or expertise to perform this type of work, members of the security team need to rely on analysis done by other external CSIRTs or security organizations. Such analysis resources may include advisories, alerts, trend analyses, and technical documents.

Vulnerability and Artifact Response Coordination

Any vulnerability and artifact response coordination that occurs will usually be within the local division or unit, to ensure that all systems in that area are addressed. Coordination outside the local unit with other parts of the enterprise usually only happens if there has been some established channel to share this information. In most cases this means that there is no comprehensive tracking and recording of vulnerabilities and artifacts across the enterprise. Without such consolidation of information, there is no mechanism for identifying similar trends or patterns, nor is it possible to identify potential new threats to the organization.

---

[38] Although the technical details are quite different, the considerations for vulnerability handling are similar to those for artifact handling. Therefore both services are handled together throughout this document. Differences are clearly stated whenever necessary.

Even if no vulnerability or artifact handling effort is undertaken, members of the security teams involved in responding to an incident or attack will need information. They might ask other CSIRTs, vendors, or security companies for assistance and coordinate any further response regarding newly identified vulnerabilities or artifacts. If a point of contact for dealing with vendors and security companies is not established, multiple parts of the organization may attempt to correspond with these vendors. This can cause confusion and in the end frustration on both parts as duplicate information is relayed through multiple channels, increasing the chance of miscommunication. Vendors may also require that only one point of contact work with them.

Development of Security Tools

Based on their involvement with the configuration and maintenance of security tools, applications, and infrastructure elements, members of a security team may experience situations in which a specific solution is not readily available. In such cases members of a security team might develop tailored tools to provide a workaround or temporary fix to help satisfy such specific requirements, if they have the necessary expertise or skills.

Other Services

Other reactive and proactive services such as incident response support, announcements, technology watch, security audits and assessments, and security-related information dissemination would not normally be provided by a security team. Of course there may be some organizational structures in which these may be provided as additional services, but in general many of these services require dedicated resources and therefore would be difficult to provide within the ad hoc nature of the security team model. Without a common focus on incident management across the organization, these services cannot be effectively provided in a coordinated manner.

4.5.3 Impact on Security Quality Management

Without the benefit of any organized response plans, it is unlikely that the security team will have the resources or time to provide any proactive quality management services that do not already relate to their normal work activities. For example, a security team will most likely not provide security awareness training, tutorials, or briefings.[39]

Since members of the security team may be involved in actually implementing and maintaining security solutions, they will likely be involved at some level in the testing of potential hardware and software products. Product evaluations can be done as part of routine purchase decisions or in response to a request by some department or unit. The evaluation mechanisms can range from informal testing to formal certifications.

---

[39] That is not to say that such activities do not occur at all, but that it is unlikely in the security team environment.

Other problems that result from the ad hoc nature of the security team include the difficulty in extracting incident trends and patterns when there is no centralized repository of incident data and reports. The CSIRT in this model is not usually positioned to provide business intelligence into any risk analysis or business continuity planning. Each member or group from the security team can try to use lessons learned from their own experiences, but other parts of the organization and perhaps even other members of the security team will miss out on the knowledge about important threats and the corresponding mitigation strategies if no coordinated exchange of lessons learned is established.

4.6 CSIRT Resources

4.6.1 Staff

This model requires no additional staffing. It utilizes existing personnel, such as system administrators, local area network and wide area network (LAN/WAN) administrators, security administrators, database administrators, help desk personnel, and software developers to support any incident handling activity at the local level. Any response efforts (reactive, proactive or security quality management) are performed in addition to the normal day-to-day responsibilities of the staff.

As the responsibility for security and incident handling resides with existing staff, their technical, communication, and personal skills determine the quality and level of response that is provided. The model does not provide a consistent method for developing incident handling expertise across the organization.

Although there are no additional salary costs incurred if incident handling tasks are done as part of the day-to-day operations of the security team, there is the potential for wasting money on duplicated and inefficient activities. Of course, if incident handling activities are outsourced, then there will be additional costs.

As with any other model it is very important to have an updated list of the staff members in the various components of the security team and their area of expertise and contact information. This information can be used to contact others when specific skills, expertise, or assistance is needed. A list of other platform or software specialists outside of the security team is also beneficial. There is no guarantee, however, that such assistance could be provided, especially if these specialists are located in other divisions, departments, or at other physical locations. They may also be too busy with their other responsibilities and tasks to provide assistance.

4.6.2 Equipment

There is no requirement for additional equipment in this model. It requires no additional ancillary support services. Existing computer equipment, peripherals, telephones, and pagers are used. If more equipment is needed for specialized analysis work, it may be possible to negotiate with other parts of the enterprise to borrow or use equipment such as software-development facilities or a test lab in a non-production environment when investigating incident activity.

4.6.3 Infrastructure

No new infrastructure costs are incurred, as there is no coordinated or focused incident handling capability. The existing infrastructure is used. It is hoped that the infrastructure will provide some computer security features, such as separate networks and firewalls, baseline computer configurations, security guidelines for system administrators, and acceptable-use policies for users. If any incident tracking or coordination is to occur at an enterprise level, an integrated help desk system will be needed that all members of the security team can use.

4.7 Summary

This model does not include a formal CSIRT. Incident response activities are handled by system, network, and security administrators throughout the enterprise who are responsible for the maintenance and configuration of the enterprise systems and networks. Incident response work is handled on an ad hoc basis as part of the normal security activities. The network, system, and security administrators involved in this work are loosely referred to as the security team.

With this model, it is critical to have well-written security guidelines, effective policies, and detailed procedures in place to ensure consistent configurations for computing environments throughout the enterprise. The constituency must rely on such defensive measures, as there is very little or no coordinated incident response team.

If incident management in this ad hoc manner is to occur with any success, some method for contacting and notifying the rest of the organization is also necessary. It is not an easy task to define where this process will reside, and even if done, whether other parts of the enterprise will respond to the notifications unless there is strong management support. One of the other internal CSIRT models would provide better coordination and management of incident activity across the enterprise.

4.7.1 Impact on Constituency

This model has the least impact on the current operations of the constituency; it is basically "business as usual." The consequences to enterprise-wide security are that vulnerabilities and risk may vary from location to location and the organization does not have the mechanisms in place to recognize threat patterns across the enterprise or the ability to prevent or mitigate such threats.

In this model, no individual or team has any real authority to effect enterprise-wide changes for the broad constituency, since the effort is focused in localized areas.

4.7.2 Constraints

The lack of a coordinated incident handling effort is the main constraint in providing this capability via the security team model. The basic problem is how to provide standard, cross-organizational reporting, analysis, and response when each division is handling those activities in an ad hoc manner.

4.7.3 Strengths and Weaknesses of the Model

As we have mentioned, one problem this model presents is that there is no way to ensure consistent and correct response across the organization. Also, viewed from an organizational perspective, by not sharing information among divisions, erroneous or incomplete recovery steps could be taken across the enterprise even if some security administrators correctly address the problem locally. Other expertise that is needed and that might exist in other units is not known, and no overall picture of the incident activity throughout the enterprise is obtained. Further, other areas of the enterprise can remain exposed to threats if the solutions are only applied where they occurred or were locally recognized and are not passed on to others.

The lack of a centralized presence or authority for incident handling and reporting also causes confusion within departments and among staff members. Staff are not sure who to notify about incidents or who to involve in response efforts. There may be such a wide variety of areas of expertise that there can be no consolidated response effort on a collaborative basis across the enterprise. In addition, some areas of expertise might not be available, leading to a situation where an incident is recognized but no one feels responsible or is able to provide the necessary support for any response effort.

A bigger problem is that it is difficult to determine ownership of a problem in this type of security environment. For example, if a UNIX system is compromised in a particular functional area, who is responsible for deciding what to do, the UNIX administrators or the functional business unit (e.g., the system operator or the system owner)? If personnel in one area discover an intrusion and suggest mitigation and recovery steps, how do they get buy-in and compli-

ance from other groups and divisions if they need their assistance? On the other hand, if one area discovers an intrusion or security breach, they may be motivated to cover up the problem before anyone else notices, rather than share the knowledge with other business units.

There are no real strengths in this model in regard to incident handling, as it does not provide true incident handling services. The only benefit gained may be that no additional costs are incurred in equipment and staffing. However, that cost savings will most probably be offset by subsequent damage resulting from incident activity that was not quickly and efficiently handled due to the lack of coordinated response efforts. It is possible, however, that a security team may be effective in a small organization, where the number of incidents are low and the team has an in-depth understanding of the systems and networks and their corresponding security configurations.

To be a successful security team in regards to incident handling activities, the following requirements are suggested. Please note that this is not a comprehensive list of everything that would be needed, but some key requirements.

- an established response plan and identified staff with designated assignments and tasks that have management support and approval

- an established method to notify the rest of the enterprise when a computer security event occurs

- a matrix or list of platform and network experts in the organization and their availability and contact information, along with support from management for them to be pulled into incident handling activities as needed

- an incident tracking system that can be shared and accessed by all members of the security team components in the organization. Included in this requirement is the need to have agreed-upon definitions, categories, and priorities for incident types.

- an identified escalation path when normal resources are not enough to handle the situation or when additional expertise and advice are needed

- security awareness training and incident reporting guidelines for the constituency and the members of the security team

5 Internal Distributed CSIRT

5.1 Overview

In an internal distributed CSIRT model, referred to as the "distributed CSIRT" through the rest of this document, the team is composed of staff from other divisions or sectors of the enterprise who report to a central CSIRT manager. The CSIRT is a formally recognized entity and has been given the responsibility for handling all incident response activities. The team is considered "internal" because it is a team within a particular organization or company, so it is internal to the enterprise. It is different from the security team model primarily because of (a) the existence of more formalized incident handling policies, procedures, and processes, (b) an established method of communication with the whole enterprise concerning security threats and response strategies, and (c) a designated CSIRT manager and team members who are specifically assigned incident handling tasks.

The CSIRT manager reports to high-level management, such as a CIO, CSO, CRO, or the equivalent. While the CSIRT manager has a "centralized" office (in organizational terms), the team members are scattered across the organization's geographic and divisional locations. Members of the team are chosen based on their experience and expertise with various operating system platforms, technologies, applications, and security practices. Team members include systems and business experts, network engineers, and others who have the needed functional knowledge.

The distributed CSIRT has full authority to analyze activities and shared authority to respond to incidents as they occur. No enterprise-wide action is taken or recommended without the approval of the CSIRT manager and possibly upper management such as the CIO. The team also has the authority for enforcing recovery and mitigation strategies with the approval and consent of the management. Divisional and functional unit managers are notified of any action to be taken in their areas and are involved in the decision-making process to determine how to implement a response.

The team has the authority to release enterprise-wide advisories and other documents, including best practices, response and recovery steps, and security updates. The team can also be involved in synthesizing and analyzing all IDS or other network/system/application logs. In a very large organization the CSIRT may only handle this type of analysis when an incident is escalated, and the initial log analysis would instead be done at a local level.

5.2 Supported Constituencies

This type of model is found in large, distributed organizations such as multinational corporations, government organizations, and educational institutions.[40] In most cases, small organizations would not be best served by this model.

5.3 Organizational Structure

There are many different ways a distributed CSIRT can be structured. The structure will depend on the size of the parent organization, the number of geographical locations where business functions are located, the number of systems and platforms supported, the number of CSIRT services to be offered, and the expertise of the existing staff.

In all structures the main function of the CSIRT manager is to coordinate the work of the distributed CSIRT. The manager should be located close to other high-level managers or the CIO/CSO, wherever the CSIRT reports. It is possible that some other members of the team may be co-located with the CSIRT manager. Depending on the work that is required, this might include some support staff or in some instances one or two analysts to help in the synthesis and dissemination of information. The CSIRT manager acts as a liaison to other parts of the organization such as upper management, human resources, legal counsel, public relations, or other appropriate groups. The CSIRT manager also is the main contact point for the team for any external organizations that want to communicate with the CSIRT. A designated backup for the CSIRT manager should be assigned and trained so the CSIRT processes can function properly when the manager is not available.

Team members are selected from existing staff and are assigned to devote a percentage of their work time to reactive and proactive incident handling issues. The percentage of effort they devote is negotiated with their supervisors and the CSIRT manager. The team members may contribute only part of their time to CSIRT work or could be assigned 100% of their time to this work. If the team members only perform CSIRT work on a part-time basis, they will report to two managers: the CSIRT manager for CSIRT work and their divisional or department manager for their normal day-to-day work. Team members can be system and security administrators, database administrators, researchers, network engineers, and any others with needed functional expertise. Other extended team members may include representatives from legal counsel, human resources, public relations, risk management, and law enforcement or criminal investigation groups. Any core or extended team members should have designated backups who have been trained and mentored to perform the required tasks and functions.

For this model to work there has to be clear understanding on the part of both management and staff that the distributed team members must stop working on routine tasks when they are

---

[40] This model especially can be found in commercial organizations with multiple sites and locations.

needed to perform incident handling functions. Usually this model works best in an organization whose distributed departments or sectors share strong common characteristics that enable them to share staff. A problem that can result in this model is that, depending on how the team is presented to the organization, it might not be viewed as being responsible for incident response across the whole enterprise.[41] Another problem that may result is that during a crisis, the distributed CSIRT staff are often put in a difficult position. Along with being responsible for their CSIRT work, they are usually experts in their own routine work. So in addition to working on CSIRT tasks during a crisis, they will be heavily used to combat the local impact of the activity. This may make it difficult for them to handle all the work necessary to resolve the crisis. Management has to prepare for this situation by ensuring other staff have been cross-trained in both the routine and CSIRT work, so that more resources can be applied when such a situation occurs.

CSIRT staff duties include helping with analysis, encouraging security awareness among those in their business divisions, and implementing agreed-upon response and mitigation strategies in their divisions. There may need to be some hierarchical delineation of the team in large organizations, which might involve supervisors for platforms, divisions, or geographic areas.

The distributed CSIRT serves two purposes: (1) it provides a broad base of expertise across all the systems in the enterprise and (2) it gives the CSIRT a foothold in each division to not only coordinate activity but promote following best practice security policies and response steps. In this way, members of the team are out in the field (i.e., local sites); they are the eyes and ears of the CSIRT. They are also the arms and legs of the CSIRT, as they will be the ones to perform the response or provide guidance to those who will be performing the response. The distributed CSIRT staff have first-hand, real work experience concerning the operations and issues facing the organization. This brings a practical view of what techniques and approaches will work to mitigate problems.

The purpose of the CSIRT manager's office is to synthesize the reports received from multiple locations to identify trends and patterns of activity, and to help identify the scope and impact of any suspicious behavior or intrusion. The CSIRT manager also coordinates the work of the distributed team members, while providing direction and guidance for the team's security policies and procedures. In some organizations the CSIRT manager may be the information security officer for the organization and as such call the distributed team together whenever an incident occurs, to perform a coordinated response.

The organization must decide how many employees from each division should be included on the team. The organization must also decide how to assign the various CSIRT services. Services can be assigned to particular individuals, groups, or departments based on their exper-

---

[41] To overcome this problem it is necessary to create an organizational image of the team as a single, tangible object, regardless of its virtual and distributed nature.

tise, job function, geographical location, or business unit. For example, incident analysis and response for threats and attacks against UNIX systems may be handled by the part of the IT department responsible for securing and maintaining the UNIX systems. On the other hand, the responsibility for handling these UNIX incidents may be assigned to the business units in which the UNIX systems reside. So if the UNIX system in question was located in the marketing department, the CSIRT team members in that department would provide the response. Another option is to have team members handle incidents for their physical location or geographic area. In this case some individual or group is responsible for all the incident, vulnerability, and artifact handling at that geographic or departmental location.

An organizational structure that can also work is to assign specific CSIRT functions to particular groups. For example, one unit might be responsible for analyzing vulnerabilities in Windows systems. Another unit might maintain a test lab for incident and vulnerability analysis, and still another might be responsible for developing and distributing communications, such as advisories or best-practice recommendations. Whatever assignments are made, staff will need training on the supported platforms.

It is extremely important that all members of the CSIRT know who has what skills and expertise on the distributed team so that they can be contacted for assistance when needed. CSIRT members also need to know when these other distributed team members are available. A shared calendar or list of operating hours and relevant points of contact for those times may be helpful. There must also be a clear notification and contact procedure that is followed when asking for assistance from other members of the team.

Communications across the team are extremely important in this model to ensure the efficient and effective operation of the CSIRT. The team will need to stay in touch through secure communications such as email, secure teleconferencing or phone conferencing, or a secure extranet or intranet. Virtual meetings should be scheduled regularly to encourage the feeling of a team working together. There should also be some type of regular face-to-face meeting, so members of the distributed team can get to know one another and share experiences or raise issues not easily addressed via phone or email. Discussion topics can also include reviewing organizational processes and procedures, service level changes or additions, strategic planning, and technical training. Management should look for ways to incorporate team-building activities into the work schedule. Ideas may include having members of the distributed staff attend conferences together or work on mock incident scenarios or other projects together. When staff members get together at face-to-face meetings, some social gathering or activity could be built into the agenda to let the team members have an opportunity to get to know each other on a more personal level to develop camaraderie.

It is important that response to a security event occurs quickly. If the lines of communication are too deep or hierarchical in structure, team members may not be able to affect an appropriate response. Some level of authority must be given to team members to act in a responsible

way within the general procedures and guidelines of the CSIRT. They could be empowered to adapt or modify procedures or guidelines in certain situations (with an after-the-fact review by management to ensure that appropriate actions were taken), discuss any lessons learned, or determine whether any policies and procedures need to be updated or added.

For the distributed CSIRT model to be successful, the following elements are required:

- There must be management buy-in and cooperation at all levels, especially from the business units where the distributed staff are located.

- The CSIRT manager must know what expertise lies in each area and determine how best to assign tasks and actions to maximize overall team success. Clear lines of responsibility and communication must be established, along with identified backups for various CSIRT assignments and functions.

- The team must understand a variety of technologies.

- There must be a vigorous effort to engage the distributed CSIRT members in team building activities.

- There must be clear policies and procedures for how incidents and vulnerabilities are reported and handled, including escalation, notification, and resolution procedures.

- There must be a shared, secure infrastructure that the team can use for communication, incident tracking, and sharing information. Information and incident activity must be pulled from all areas of the organization and synthesized to provide an enterprise-wide view of security problems, incident trends, and response strategies.

5.4 Triage

In a distributed CSIRT, the triage process is important for providing an understanding of the scope of the reported incident activity. Organizations adopting the distributed model must also decide where to locate the reporting function for the CSIRT both physically (geographical and building location) and organizationally (department or division) within the enterprise. Various options exist, as described in Section 3.3.1, Triage.

The main decision point in this model is whether all reports come in to the CSIRT manager's office, either through a CSIRT help desk function within that office or a centralized organizational help desk, or if reports will first come into the local level to the distributed team member.

If reports come in centrally, the CSIRT manager will determine where the incident should be sent for analysis and response. A predetermined contact list of distributed team members and their locations, skills, and technical responsibilities is used to make the decision concerning where to send the reported incident.

If reports come into the local level and the triage process is done by the distributed team member, they must ensure that the report and any response is added into any incident tracking system and that the CSIRT manager is notified of the activity in case further actions are required throughout the enterprise.

The key in the distributed model will be to ensure that all incident activity is collected and tracked by the CSIRT manager's office, so that the impact and threat across the enterprise can be determined and also so that any trends and patterns can be identified. An incident tracking system accessible to all members of the distributed team will be required so they can update the status of or review any incident being handled at the local level. This shared system will provide the CSIRT members with access to incident information across the organization that may provide insight, warnings, or remediation strategies that may be useful at the local level. The incident tracking system should have the capability to allow different team members to record the distinct actions they have taken to analyze and resolve problems, particularly if different people will be working on the same incident.

5.5 Available Services

The following sections describe the types of CSIRT services that might be provided in a distributed CSIRT model. It is recognized that every team is different, so these are general descriptions based on observations of and discussions with other teams. The method in which the services are delivered assumes a certain level of infrastructure, staff, and equipment. These are described later in this section.

5.5.1 Core Services

The following tend to be the basic services provided by a distributed CSIRT. They are somewhat different from the baseline core services discussed in Section 2.7.4.[42]

Alerts and Warnings

In a distributed model, all alerts and warnings coming into the CSIRT or parent organization from other security experts, vendors, or CSIRTs are received by the CSIRT manager or his or her designee. From there the alerts and warnings are disseminated to all members of the distributed team. Team members pass on the alerts and warnings to other system and network administrators, business managers, or security teams at their sites. General alerts and warnings that affect all members of the constituency are sent to a predetermined mailing list by the CSIRT manager or their designee. For this service to work efficiently there must be an up-to-date list of people and units to notify. This list should be maintained by the CSIRT manager with input from all the relevant areas where distributed team members reside. Input should

---

[42] As previously discussed, your individual experiences or needs may differ.

also be collected from any newly defined areas or departments or constituency groups in the enterprise. This list must be verified and updated on a regular basis.

If alerts and warnings for the CSIRT's constituency need to be developed, these are assigned by the CSIRT manager to the individuals of the distributed team with expertise in the technology and mitigation strategies that need to be discussed in the alert or warning. Even if the alert or warning is developed in another part of the distributed team, it should be reviewed and possibly sent out from the CSIRT manager or his or her designee. There may be a need to work with a technical writer to produce the final versions of the alerts and warnings. If a technical writer is not on staff as part of the CSIRT, it may be possible to use staff with the needed skills from the constituency or parent organization. Whatever method is used to obtain technical writing assistance, this arrangement should be established in advance, so that the technical writer can be called upon as needed.

Incident Analysis

The distributed team members focus their analysis on the affected systems in their area of responsibility. The CSIRT manager's office correlates the incident activity across the enterprise to determine the scope of the activity, the impending threat, and the response effort required. The CSIRT manager's office also analyzes any reports to determine any intruder trends or patterns. Based on its understanding of the overall picture, the CSIRT makes recommendations for strengthening security across all of the organization's systems.

Incident analysis is performed by the members of the team who have expertise in the functional area, operating system, network, or application software involved in the incident. For newly reported attack types, the distributed team can collaborate on the investigations, pooling resources and expertise across the enterprise to help identify, analyze, and develop recovery measures.

Incident Response Support

The main focus of the distributed CSIRT is on providing the incident response support and guidance necessary to analyze and respond to incident activity. In most cases the distributed team members work with system and network administrators at the local level to help them respond to incidents, rather than performing the repair and recovery work themselves, as they would if they offered on-site incident response services.[43]

However, it is true that in some organizations, the distributed team members themselves are the system and network administrators and may actually perform the incident response tasks. Because this is not always the case, however (since some organizations use security officers or information security officers as their distributed team members and these people are not usu-

---

[43]   It is possible that the distributed team may indeed be structured to provide on-site response, as discussed under "Additional Services" below.

ally network and system administrators), the on-site incident response service is included in the next section, "Additional Services."

Incident Response Coordination

Coordination is handled initially by the CSIRT manager of the distributed CSIRT. This includes keeping each part of the distributed team up to date with the latest information, distributing information about the impact and scope of ongoing incident activity, and providing guidance for response strategies during events.

The CSIRT manager or designee is the main point of contact to coordinate any information dissemination or collaboration with upper management, the organization's legal counsel, human resources, law enforcement, or other internal parties unless organizational policies dictate that someone else must be that point of contact.

If other external parties such as victim or source sites, other external CSIRTS, or other security experts need to be contacted, the CSIRT manager or designee would also be responsible for orchestrating those interactions as appropriate, unless organizational policies determine someone else as the external point of contact. Those performing the triage function would act as an initial point of contact for such communication as well and pass information on to the appropriate team member.

In this model, CSIRT procedures are in place to escalate events to higher management, coordinate with public relations, or pass security events to law enforcement or other investigative bodies for criminal investigation as needed. The distributed team members understand the guidelines and serve as the points of contact for routing information to others in their division or geographical area as appropriate. Enterprise-wide messages, alerts, and advisories are sent from the central CSIRT office, upper management such as the CIO, or even public relations.

Because there is a coordinated triage function, information from across the enterprise can be reviewed. This allows the team an opportunity to identify any security gaps and determine the scope and potential impact of the reported activity. By seeing all the activity, the CSIRT can more easily prioritize and balance the workload. They are also able to predict or head off potential problems. For example if a virus is spreading across the network in one geographic area, it could be identified and stopped by proactively taking steps before it affects another geographic area.

Although there is information sharing among the CSIRT's members, without a focused and energized CSIRT manager, strong management support from divisional supervisors, and some quality assurance testing, there is no good way to ensure that all members of the team are reacting appropriately to assigned tasks. With a large, distributed organization, there must be a way to check that response steps are handled in a consistent manner. There must also be a fol-

low-up mechanism in place to ensure that all response steps were implemented at each site as directed. Supervising these follow-up functions is one of the duties of the CSIRT manager. There will need to be sufficient resources to allow such work to occur.

Vulnerability and Artifact Response Coordination

If any vulnerability or artifact response coordination is undertaken, it is handled in a manner similar to incident response coordination. Information on the analysis and mitigation strategies and response efforts regarding any vulnerabilities and artifacts is consolidated at the CSIRT manager's office for dissemination to the rest of the team. For the most part, the actual analysis of any artifacts or vulnerabilities is done by the members of the distributed team with technical expertise in the affected operating systems and software, but it may also be done by an outside source such as a vendor or other external CSIRT. Whoever does the work will then pass their analysis or remediation strategies to the CSIRT manager for dissemination.

Because of the distributed CSIRT structure, even if vulnerabilities and artifacts are found on systems in one part of the organization, the analysis and response can involve team members from other geographic or departmental areas who have expertise to handle the required tasks. This coordination and any assignment of tasks is orchestrated by the CSIRT manager.

Even if no vulnerability or artifact response effort is undertaken by the distributed CSIRT, the team will still need information about any vulnerabilities or artifacts found in their systems. They will most likely look to other public or private information resources to get this information. This may mean getting alerts, advisories, or mitigation strategies from other external CSIRTs, vendors, or security companies. The CSIRT manager is the initial point of contact for work with other entities, but other distributed team members may be involved when their expertise is needed.

Announcements

Announcements are developed by the CSIRT manager or by assigned team members based on the topic and the team member's relevant expertise. Most often they are disseminated from the CSIRT manager or passed on to upper management or public relations for broadcasting. Assistance from technical writers may be required to ensure quality and understandability.

5.5.2 Additional Services

In addition to its core services, a distributed CSIRT may choose to offer other services. The following services are those most likely to be provided.

Incident Response On Site[44]

Since the distributed team members are located at various sites throughout the organization, and since they may actually be the system and network administrators at these sites, it is possible to have them perform the actual response. This service can only be provided if the distributed team members have the requisite skill set and the available time.

The distributed team members still receive directions and guidelines from the CSIRT manager, but would also need to have some level of authority to take appropriate actions during emergencies or when the threat is immediate. It is very important that the distributed team members pass all information gathered and all steps taken during an incident on to the CSIRT manager. Conversely, when the CSIRT manager's office disseminates a set of response steps or strategies to be implemented, the distributed team members need to confirm that they have executed the response correctly.

Vulnerability and Artifact Analysis

If this service is provided, it will probably be done on an ad hoc basis, initiated by a real need when artifacts are found on compromised or infected systems, or when a vulnerability is found in software supported within the organization. In a distributed team model, CSIRT staff members usually do not have the time or expertise to do this type of work for general research purposes. Distributed team members can, however, engage in vulnerability and artifact analysis to determine what impact any new vulnerabilities or found artifacts have on their infrastructure.

Whatever analysis is done, there must be some way to record and track the vulnerabilities and artifacts analyzed and the response that was taken to handle them. The CSIRT can also choose to store the artifacts found in some type of archive. In this way, any new artifacts can be compared against those in the archive to determine if they are similar or new, what they signify, and how to handle them.

Staff performing this service are required to update the rest of the CSIRT with the information discovered through their analysis. This helps other parts of the team perform the appropriate response if their systems are also threatened.

If analysis is not done, information about vulnerabilities and artifacts is obtained from other entities such as other external CSIRTs and security experts, as described under "Vulnerability and Artifact Response Coordination" in Section 5.5.1.

---

[44] This service is not included under core services because many teams only perform a support or co-ordination role and do not do on-site recovery and repair of systems. However, since some teams do provide this service, we've included it here.

Vulnerability and Artifact Response

Just as in incident response on site, vulnerability and artifact response can be performed by the distributed team members at each organizational location. Again the staff needs to have the required expertise and understand supported platforms for the local site or across the enterprise.

If staff perform this function, they determine the appropriate actions to detect and remove artifacts found on systems. They search for and patch vulnerabilities. The CSIRT manager or other team members with the necessary expertise provide guidance.

In addition, distributed team members may take protective measures to avoid similar future attacks and incidents. This usually involves implementing secure configurations, updating or creating virus signatures that can be added to virus scanning databases or intrusion detection systems, and keeping operating systems up to date with new versions and patches.

If this service is not handled by the CSIRT, it is most likely handled by the organization's IT department, security team, or through a contracted managed security service provider (MSSP). The CSIRT will require established channels of communication to interact and share information with any other group providing this service.

Technology Watch

If done, this service is probably only performed at a cursory level, depending on available time and resources. If members of the distributed team have other work duties, they may not have time to work on a technology watch function.

If this service is performed, there are several ways it can be provided. In the more centralized method, the focus for this function resides with the CSIRT manager's office. This may mean that an additional staff member is needed in this office. In a more distributed method, one area of the team can be assigned this function as a full-time responsibility. Another distributed method is to have some members of the distributed team assigned to stay current on information in their area of expertise, such as a particular operating system, architecture, or function (IDS, firewalls, etc.), and designate one or more team members to consolidate the information from the other team members.

No matter what the method, staff members assigned to perform this watch function do so by monitoring newsgroups, mailing lists, other advisories, alerts, etc. Information from other members of the team in the divisions and sections is forwarded to the CSIRT manager to be consolidated and disseminated throughout the team. Collecting this information from distributed CSIRT staff members gives a more comprehensive overview of information from people with expertise in various applications, operating systems, protocols, and tools. More impor-

tantly, it reduces the duplication of effort so that all team members aren't reading the same set of resources.

This consolidated information highlighting current attacks, threats, response steps, and work-arounds is made available to team members via the secured intranet or extranet.

Security Audits or Assessments

With its technical expertise and experience handling new vulnerabilities, real incidents, and artifacts, the distributed members of the CSIRT could participate with an audit or assessment team in the provision of this service, or provide input into the development of compliance criteria and requirements.

However, it is important that the involvement of the CSIRT does not create a conflict of interest. Team members should not audit their own systems and networks or their own division's systems and networks. They must also be objective and diplomatic, so as to create a level of trust between the CSIRT and the system and network administrators who maintain the hardware, software, and perimeter defenses. The goal is to have the system and network administrators feel comfortable in accepting guidance and recommendations from the CSIRT or any other auditing or assessment group.

Configuration and Maintenance of Security Tools, Applications, and Infrastructures

In most organizations, responsibility for configuration and maintenance of security tools, applications, and infrastructures falls to the IT department or designated network or security administrators. Although security infrastructure elements such as firewalls and IDS are sometimes placed within the responsibility of the CSIRT, this should be avoided, where possible, to allow the team to focus on incident management rather than maintenance.

However, it should also be recognized that if the CSIRT is not responsible for these types of services, the team's expertise and experience with security tools may be useful in providing advice and guidance to the organizational staff who are assigned to these functions. Establishing a good working relationship with system, network, and security administrators and the IT department will help make any necessary response efforts that require changes to systems, firewalls, or network logging smoother and more efficient.

If the distributed team members do not perform CSIRT work 100% of the time and have other assigned duties, it may be the case that they perform these configuration and maintenance tasks as part of their normal job functions.

Development of Security Tools

Based on their involvement with the configuration and maintenance of security tools, applications, and infrastructure elements, members of a distributed team may experience situations in which a specific solution is not readily available. In such cases members of a distributed team might develop tailored tools to provide a workaround or temporary fix to help satisfy such specific requirements. This development work can occur only if they have the necessary expertise or skills, and will be an outgrowth of their practical experience with the systems. Coordinating such developments with the rest of the CSIRT is important so that other parts of the organization can benefit from the results.

Intrusion Detection Services

If the intrusion detection service is not provided by the IT department, it can be provided by the distributed CSIRT. In this case the IDS is set up in each relevant division, ideally under the management (or supervision) of a member of the distributed CSIRT. Information is gathered in a standardized fashion and passed to the CSIRT manager's office for review, consolidation, analysis, and appropriate response. This ensures that patterns of activity across the enterprise are analyzed and responded to in a comprehensive manner.

One part of the distributed CSIRT may also be given the assignment to review all IDS logs, synthesize the results, and disseminate any alerts on abnormal activity to the relevant area of the team for investigation, analysis, and response.

Security-Related Information Dissemination

The CSIRT can establish a centralized web site (and if appropriate FTP site) to provide organization-wide access to appropriate security-related information. They can also use these sites to disseminate information from other external sources that has been tailored to the needs of the constituency in regard to supported technologies and software. Information can also be distributed via newsletters and mailing lists. This may be a difficult service to provide depending on the available staffing resources. If done, it may be at a minimal level only—making available copies of patches and security alerts.

Unless a particular set of team members is assigned the task of maintaining any of these broadcast mediums, the CSIRT manager's office will most likely be responsible for synthesizing any information for release. Information can be collected or written by CSIRT staff during any free time they may have or as a particular assignment. This provides team members a chance to be involved in other activities and provides a change from their routine work assignments.

Information disseminated includes current activity reports, threat trends and patterns, security awareness tutorials, incident reporting forms and guidelines, current updates on CSIRT devel-

opments, and any special security-related information on various applications, protocols, and security or attack tools.

Maintenance of this CSIRT site can be the responsibility of one set of team members or the CSIRT manager's office. If the CSIRT manager's office takes the responsibility, additional staff may be needed to handle the update and maintenance functions.

If the CSIRT site is not maintained by the team but by other parts of the IT group, then it will be important for the CSIRT to work closely with the administrators to ensure the server is adequately protected and that information is updated in a timely manner.

5.5.3 Impact on Security Quality Management

The amount of time that can be devoted to security quality management services will depend on the resources available from the distributed team members. In most cases, the CSIRT manager may provide input into these initiatives. Distributed team members with functional expertise, can be pulled into initiatives as time permits.

Distributed team members are responsible for promoting security awareness at their sites. They can do this by holding briefings, tutorials, or brown bag lunches to make relevant information or documentation developed by the CSIRT available to the organizational divisions.

The CSIRT will likely be asked for input in regard to implementations and maintenance of security solutions. This, as well as the expertise of CSIRT team members, can lead to the team's involvement in testing potential products. This can be done in various ways, from informal tests to formal evaluations. The testing can occur across the enterprise or can be done in response to a request by some department or unit. Based on their skills and knowledge, the CSIRT could also be involved in the development of business continuity and disaster recovery plans or could assist in the provision of security audits and assessments.

5.6 Resources

The following staff, equipment, and infrastructure resources should be considered when implementing a distributed CSIRT model.

5.6.1 Staff

The distributed CSIRT comprises a small, centralized management staff and team members who are spread across the organization:

- CSIRT manager (reports to the CIO or other high-level manager)

- one or more system administrators for the CSIRT infrastructure (dedicated or part of existing IT service)

- one or more administrative support person(s)

- one or more analysts (depending on the services offered, these analysts may help synthesize incident statistics, IDS data, security alerts, and technical documents)

- distributed team members (number determined by parent organization based on the size of the constituency being served and the services provided)

The distributed CSIRT calls upon other adjunct staff that may be assigned to the CSIRT on an as needed basis, such as

- technical writers

- trainers and instructors

- public relations staff

- legal counsel and criminal investigators

- other technical experts (administrators, managers, Windows/UNIX/mainframe experts)

For this model to work effectively, pre-arranged agreements will need to be established for how and when this additional staff can be called upon to provide assistance.

The services provided by the CSIRT are determined by the skills of the existing system, network, and security administrators in the organization and the requirements of the enterprise. It is expected that such skills would include, for example, hardware and software expertise in whatever technologies and functional business systems are supported throughout the constituency, including any systems, software, and applications developed in-house.

All members of the team need training on the operation and purpose of the CSIRT, along with technical training in normal incident handling activities. Backup staff should be identified in each unit where a distributed team member works so there is one backup for CSIRT work and one for the team member's regular, non-CSIRT duties.

A method for holding CSIRT meetings for all distributed staff is necessary to encourage a true team attitude. This may be done via a secure teleconferencing system or even an extranet. Periodically, face-to-face team meetings (where feasible) should be held to help the team get to know one another. This can be done at training classes or special off-site sessions. Of course, there should be a system of backup personnel to perform CSIRT functions while the team members are meeting.

The parent organization should promote distributed CSIRT positions as highly desirable and emphasize that such team members play an important role in the overall computer security

infrastructure. These positions should be recognized and compensated appropriately. CSIRT distributed staff will gain a wider range of skills and experience from their involvement on the team. This can be a useful selling point for getting their home department or unit to give approval and support for their participation on the CSIRT.

If compensation for the added responsibilities associated with serving on the team are in the form of supplemental payment, this will of course mean that additional salary costs will be incurred. This does not include costs for charge-back of other adjunct staff. Overhead and other fringe benefits need to be considered as well.

The organization can also choose to outsource some of the response capability to a third-party contractor. This service can be provided as a recurring cost or on a fee-based schedule, depending on a number of factors, including the type of organization, sponsor, or service requested. For a distributed team, the third-party contractor would either provide human resources to augment the distributed CSIRT or cover services such as advisories, alerts, or IDS monitoring to reduce the team's workload. The main responsibility for decision making should rest with the organization, however, not the contractor.

5.6.2 Equipment

The distributed team members use existing computer equipment, peripherals, telephones, pagers, and other equipment. Staff can negotiate for the use of other equipment for testing if it is not available in their area. Additional equipment can be appropriated through the CSIRT manager and/or other financially responsible individuals. Access to a secure intranet or other communications mechanisms will also be required.

It is possible that if there is any additional staff located with the CSIRT manager, some additional equipment will be required. This could include (but is not limited to)

- office space and furniture (supplies, copier, etc.)
- computer equipment for day-to-day operations and activities
- telecommunications systems, including stationary and cell phones, and pagers if appropriate
- home equipment and remote access, if appropriate

5.6.3 Infrastructure

The distributed CSIRT infrastructure should include access for all distributed team members to

- a secured incident report tracking system
- a secured repository for archiving all incident and vulnerability artifacts, such as exploit scripts and toolkits

- secure communications channels, such as secured email, phones, video conferencing, faxes, intranet, or extranet as needed

It should also provide

- physical security

- protected power sources

- network and host security

- ideally, a separate CSIRT network for shared systems with a secure configuration and firewall, as well as VPN access for distributed team members

- secure backups and storage of CSIRT data

- mechanism for updating software and patches

- virus protection and scanning

- web tools

- encryption technologies

Depending on the systems used, this infrastructure might require special client/server hardware and software at team locations and the CSIRT manager's office.

5.7 Summary

This model staffs the CSIRT by assigning responsibilities to designated individuals across the enterprise. These individuals become members of a distributed "virtual" team. The distributed CSIRT has a manager and may also have a small support staff located with the manager.

5.7.1 Impact on Constituency

The distributed team in essence becomes a conduit for collecting information across the enterprise and using this information to formulate strategic plans for securing the infrastructure and responding to any incident activity. The distributed team also provides a channel for disseminating alerts and advisories outlining preventative measures to take to protect the infrastructure along with disseminating any response measure for intruder activity. The distributed team members can also act to ensure that the appropriate steps have been followed. They can provide this information as feedback to the centralized team.

This model has several major impacts on the constituency:

- Each organizational entity must be responsible for continually providing the appropriate resources (people with the right skills and experience, authority, access, etc.).

- An infrastructure (described above) must be provided to support the team.

- Effective management of this team will require coordination across many parts of the organization and vigorous efforts to involve all members of the distributed CSIRT in team-building exercises.

- Technical incident training and mock exercises should be conducted and supported to maintain proficiency.

- Methods must be established to allow information sharing among the team members so they can learn from and act on one another's data and experiences.

There are also possible impacts on the security of the organization or constituency. With a coordinated, distributed method for collecting and analyzing data and performing response, a better picture of the preparedness of the overall organization should be seen. Also, response time should be quicker and response efforts more consistent, ultimately leading to lower response and recovery costs, less damage from security incidents and a more secure environment.

This distributed CSIRT model represents a modest approach to the infrastructure investment required to begin collecting and analyzing security threat patterns throughout the enterprise. It provides a virtual network for the identification of threats and vulnerabilities, the dissemination of security information and the implementation of a coordinated response plan for managing incidents and threats. It is an improvement over the security team model.

5.7.2 Constraints

The main constraint for this model involves enabling the team to function as a whole when members are separated across geographic and organizational locations and administrative/management domains. Such separation can create many logistical problems. These problems include

- having staff with differing levels of expertise across the organization who may not implement a response action in a consistent manner across the enterprise

- not being able to coordinate information across multiple sites and people

- possible conflicts in the prioritization and support of distributed team members' CSIRT work by management

- possibly not scaling well in very large, geographically dispersed organizations

Because of these constraints, it is essential to have an effective CSIRT manager who works well with other division and organizational managers and is able to coordinate and supervise team assignments. The manager must be able to negotiate for additional resources when needed. The CSIRT manager's ability as a negotiator and ambassador are paramount to the success of this model. Organizations constantly reorganize; managers and units come and go.

A major overhead for the CSIRT manager will be the constant update of who in the business units they need to work with to ensure they have access to appropriate staff. The larger the number of dispersed team members, the more difficult it will be for the manager to negotiate with all the involved organizational units.

If the distributed parts of the organization are located in separate affiliated companies or in other countries, there may also be difficulties in coordinating actions because of differences in languages, laws, policies, procedures, and time zones.

5.7.3 Strengths and Weaknesses of the Model

In this distributed model the responsibility for incident handling is assigned to appropriate individuals across the organization. With the proper software, training, and equipment, this model can provide incident reporting and incident analysis, and serves as a vehicle for formulating and deploying effective responses across the organization. By having such a coordinated process the organization is able to set policy, enforce standards, and implement incident handling activities enterprise-wide. Because the distributed team is composed of operations personnel at various locations, these individuals are very attuned to local operations and conditions. This close association with local operations can provide valuable input to the development of practical policies and procedures.

This model does have its weaknesses, especially if the team is composed of staff that have split responsibilities. Finding individuals with the appropriate experience, skills, and training who are willing and able to take on additional responsibilities may be problematic. Once found and trained, these individuals must be allowed to invest the time and energy to keep their skills and abilities current. If this does not happen then the appropriate commitment from the operating units may not be sustainable over time. Consequently the required skills and capabilities may not be available when they are needed most. This makes the incident handling capability only as good as each part of the distributed team. Also, effective management and coordination of the distributed team may become a problem, without a strong leader and appropriate upper management support.

The strengths and weaknesses of this model can be summarized as follows:

- Strengths
  - There is a focused responsibility for performing CSIRT services.
  - The capability exists to coordinate incident reporting, analysis, and response across the organization.
  - There is a centralized tracking system and a centralized repository of incident data.
  - A consolidated and comprehensive view of the vulnerabilities and incident activity across the enterprise can be developed and any trends or patterns identified.

- Staff is available at the divisions or functional business units to enact response steps or provide information and expertise in their relevant fields.
- Since the CSIRT staff members are located within the divisions and functional business units, they understand the systems and software at those locations. They will have first-hand knowledge in some cases of the organization's IT infrastructure and will know what components are critical to the infrastructure. The CSIRT staff bring a unique, practical approach to the real-life operation of the organization and will understand what strategies are going to be effective and viable.

- Weaknesses
  - Experienced staff may have commitments that prevent their participation in distributed team activities.
  - Existing staff may not have the required security training or expertise. Finding experts in the organization can be difficult, and over time there can be problems with turnover and training issues.
  - Staff members may be unwilling to take on the additional responsibility unless they perceive some value in the work that is being performed or receive additional compensation.
  - Determining where the CSIRT authority lies and the willingness of other divisions and functional units to accept that authority can be difficult.
  - Keeping the staff up to date with new technologies is difficult.
  - Keeping communications current and timely across a large, geographically dispersed area is difficult.
  - Verifying that CSIRT response efforts are implemented consistently across the enterprise can be difficult and time consuming.
  - Keeping the list of staff and their areas of expertise up to date is a difficult task for the CSIRT manager without the cooperation of the distributed team members and other groups within the organization.
  - If the organization is very large and crosses multiple time zones and countries, this model may not scale.

6 Internal Centralized CSIRT

6.1 Overview

The internal centralized CSIRT model is a dedicated CSIRT, centrally located, that has full responsibility for all incident reporting, analysis, and response. In many cases team members spend 100% of their time working for the CSIRT and perform all incident handling tasks. There is a CSIRT manager who reports to high-level management such as a CIO, CSO, or CRO. All CSIRT resources are located at a central site. This model is referred to as the "centralized CSIRT" throughout the rest of this document.

This model provides a centralized team that can collect information from a wide variety of constituent sources and quickly synthesize and disseminate it across the enterprise. The CSIRT responds to reports of abnormal activity or other incident reports. It can also participate in incident and vulnerability analyses, lend expertise in testing or assessing the security of the enterprise, and play a proactive role in promulgating computer security awareness and training throughout the organization, if appropriate to the organizational structure.

The centralized CSIRT has full authority to analyze activity and full or shared authority to respond to incident activity as it occurs. No enterprise-wide action can be taken or recommended without the approval of the CSIRT manager and possibly upper management. The team also has the authority to enforce recovery and mitigation strategies with the approval and consent of upper management. Divisional and functional unit managers are notified of any action to be taken in their areas, and are involved in the decision-making process to determine how to implement a response.

The team has the authority to release enterprise-wide advisories and other documents, including best practices, response and recovery steps, and security updates. The team can also be responsible for reviewing and analyzing all IDS or other network/system/application logs.

The organization determines whether the CSIRT will visit victim sites in the parent organization to enact response efforts or whether they will recommend responses to be carried out by the local system, security, and network administrators in each division.

6.2   Supported Constituencies

This model can be used by two very different types of organizations. It is most commonly found in small organizations, where the number of staff, systems, and buildings can be handled by a small centralized IT department and CSIRT. An example might be a small commercial organization, one government department or agency, an educational institution, or a vendor organization.

The model can also be implemented in a larger organization with a constituency dispersed over many different physical and geographical locations. This type of organization might be a large educational institution with many branch campuses or a military or government organization with many departments.

In all of these cases, whether a large or small organization, the constituency itself has some common characteristics and a common organizational structure that allows the CSIRT to work with the different business units or groups.

This model can also be used, but with some difficulty, in a large organization with multiple affiliate or subsidiary companies or groups. An example might be a large multinational corporation that is comprised of a collection of independent legal entities (affiliates and subsidiaries). In this case, although seen as part of the same parent organization, each affiliate or subsidiary might have its own management structure, policies, procedures, and authority, or even its own CSIRT. This may cause problems in how much authority the centralized CSIRT has over the systems, networks, and incident response efforts in the affiliates and subsidiaries. This may also cause problems in effecting a consistent level of response across these disparate units. Although a centralized CSIRT can work in this organizational situation, a coordinating model might be a more effective approach. It should be remembered that in a commercial organization, business impacts are the crucial decision criteria, so usually the CSIRT provides advice rather than dictating the actions to be taken.

This model can be implemented but will not work as well for a large, dispersed, diverse constituency, such as numerous countries in a particular geographic area or numerous educational or commercial entities in a country. In those types of organizational settings, a coordinating CSIRT, described in Section 8, is a better organizational model choice.

6.3   Organizational Structure

The centralized CSIRT should be comprised of staff with expertise in all systems and platforms supported by the enterprise. If this is not possible, experts in the parent or host organization must be identified to work closely with the team as needed. The CSIRT manager reports to the CIO, CSO, CRO, or other equivalent manager and represents the CSIRT on boards,

councils, and activities that involve or are related to computer security. The team is centrally located at one physical site, close to their upper-level manager.

A centralized team's services can be organized in a variety of structures. The team can provide a full range of incident handling services or just limited services, such as only intrusion detection, or only incident analysis and response coordination. It is up to the parent organization (or constituency) to decide what services will be provided. A centralized team in a large, geographically dispersed organization cannot reasonably provide direct incident response on site, but it can act efficiently in providing incident, vulnerability, or artifact response coordination services, such as providing advisories, alerts, training sessions, and documented procedures.

Generally the centralized CSIRT staff perform incident handling and CSIRT tasks 100 percent of their time. However, in some instances, due to budget constraints, it may not be possible to have all full-time centralized team members. Instead there may be a core set of assigned staff who share responsibility for CSIRT functions. So there is always someone on the centralized team, but each staff member rotates on and off the team periodically. This type of part-time staff may work well in a very small organization where the CSIRT staff members also perform other IT or security-related tasks.

Another organizational option is to outsource part of the CSIRT work to a third party contractor to augment the CSIRT's expertise and provide specific support such as the development of alerts and advisories or the monitoring of IDS logs. Organizations should take great care when opting to outsource any of their incident handling tasks and functions. Issues related to CSIRT authority, data protection, information disclosure, and securing the incident handling infrastructure as it pertains to the outsourced functions must be addressed. Guidance for outsourcing managed security services is available in *Outsourcing Managed Security Services* at <http://www.cert.org/security-improvement/modules/omss/b.html>.

6.4 Triage

In a centralized CSIRT, the triage function is essential to the operation of the team. There is an established method for contacting the CSIRT such as an email alias or phone number. This method of contact is used for not only reporting incidents but also for making other requests for CSIRT services. CSIRT service listings, hours of operation, and incident reporting guidelines are widely advertised so the constituency understands how to interact with the team. There are online reference materials to assist the organization's staff in reporting to and contacting the CSIRT.

In this model, triage can be provided through two different structures: as a component part of the CSIRT or as a separate entity from the CSIRT. These two approaches are outlined in Section 3.3.1.

Whatever help desk or hotline approach is used, it is also important that the constituency understands the organizational security policies and procedures. All users must understand the importance of reporting attacks, viruses, and any other suspicious or abnormal activity. There must be no fear of retaliation for reporting activity to the help desk. Guidance for reporting activity is available to the constituency via an intranet or some similar application.

Because the centralized reporting and triage processes provide a way to coordinate the collection of information, it is possible to know what type of activity is being observed or reported across the organization. The CSIRT can therefore identify in a more efficient and timely manner whether critical system and network services are being attacked.

6.5   Available Services

The following sections describe how some CSIRT services might be provided in a centralized CSIRT model. It is recognized that every team is different, so these are general descriptions based on observations of and discussions with other teams. The method in which the service is delivered assumes a certain level of infrastructure, staff, and equipment, which are discussed in later sections.

6.5.1   Core Services

The core services characterizing this centralized model are very similar to the core services for a distributed CSIRT listed in Section 5.5.1.

Alerts and Warnings

In a centralized model, all alerts and warnings coming into the CSIRT or parent organization from other security experts, vendors, or CSIRTs are received by the centralized team through some designated point of contact such as a CSIRT phone number or email alias. From there the alerts and warnings are disseminated to various points of contact throughout the organization, which might include system and network administrators, business managers, or security teams at their sites. In this way a common message with a consistent set of steps to prevent or respond to any activity or security incidents can be sent throughout the organization. General alerts and warnings that affect all members of the constituency are sent to a predetermined mailing list by the centralized team. For this to work efficiently there must be an up-to-date list of people and units to notify.

It should be noted that members of the distributed team also may receive alerts and warnings from external sources such as security mailing lists and advisory lists. Just because the centralized team is the designated point of contact does not preclude the distributed members from obtaining information from other sources. In many cases, where threats are immediate, distributed team members may not want to wait for the information to be re-sent to understand

about new attacks or problems. However, the responses taken should be coordinated with the centralized team and any information that the distributed team members receive that is not received by the centralized team should be passed on.

If alerts, warnings, or advisories for the CSIRT's constituency need to be developed, these are assigned by the CSIRT manager to a member of the centralized team. The assigned staff can enlist the help of others in the organization who have expertise that might be needed. They may also want to work with a technical writer to produce the final versions. If a technical writer is not on staff as part of the CSIRT, it may be possible to use staff with the needed skills from the constituency or parent organization. Whatever arrangement is used to obtain technical writing assistance, it should be established in advance, so that the technical writer can be called as needed.

Incident Analysis

Because centralized team members have dedicated time to spend on CSIRT work, they often can perform more proactive incident handling functions such as analyzing incoming reports and identifying any trends or patterns appearing across the organization.

Based on its understanding of the overall picture, the CSIRT makes recommendations for strengthening the security of the enterprise systems, similar to how a distributed CSIRT works. But because team members are physically located together, the team can more easily discuss incident activity to determine similarities between incidents. This close proximity and interaction can potentially decrease the amount of time it takes to determine the scope and nature of an attack.

However, because of the centralized nature of the team, the CSIRT staff may not know a lot about the real infrastructure of the organization and the practical day-to-day issues of business needs versus risks. Therefore, they may have to involve other parts of the organization in their analysis of any incident activity, especially in regards to acceptable response and mitigation strategies. Part of the training that any centralized staff will need to receive is an understanding of the critical systems as they relate to the parent organization's missions and goals. The CSIRT staff will not be able to operate in isolation; they must spend considerable time learning about the enterprise infrastructure, organizational business goals, and critical assets and establishing good channels of communication with other parts of the organization.

Incident Response Support

This service is especially prevalent when the constituency is a large, dispersed organization, because the CSIRT can serve as a focal point for disseminating information and response strategies. To be successful at this service, the CSIRT must have a good collaborative working relationship with the other parts of the enterprise.

In its role as the centralized CSIRT, the team is responsible for initiating the appropriate response and recovery steps based on the reports received and the analysis done. Because team members' time is devoted to CSIRT work, they can consolidate and distribute information in a more timely manner. They usually also have a broader perspective on security issues and more in-depth incident handling skills. This allows them to better understand the technical nature of threats and risks (real or potential) and to provide direct guidance on recovery actions to assist local administrators.

Response can be implemented in a number of ways. In larger organizations, the CSIRT can be responsible for sending out technical guidelines on how to handle or recover from a particular security event. These guidelines are received and followed by system, network, and security administrators or other responsible personnel in each division. The guidelines are also sent to the division and business unit managers so they are informed. In this model, as with the distributed model, it may be difficult for the centralized CSIRT to determine if the correct response effort has been taken at the division level. Some means of ensuring consistency and accountability should be implemented. One problem is that even though the centralized team can work closely with the administrators in the field to explain response strategies, they do not have the face-to-face contact available through on-site incident response.

In a smaller organization, the CSIRT may actually be located in the same physical area as the system and network administrators responsible for implementing the response. This can make it easier to establish strong working relationships with these administrators, which can in turn enable a more efficient response effort.

In larger organizations, however, there may be times when the CSIRT staff is not able to react to an immediate threat as quickly as is needed by the part of the organization having a security problem or incident, and the local system and network administrators must take action themselves before involving the CSIRT. Some "rules of engagement" should be established in advance for these kinds of cases. It will be especially important in such instances that the local system and network administrators report to the CSIRT as soon as possible about what triggered the activity and what action they took to respond to the event.

Incident Response Coordination

Their central location and ability to gather and synthesize information from across the enterprise establish the CSIRT as the best point for incident response coordination. They have the information and the expertise in incident response. In this capacity they are able to act as a point of contact regarding incident activity with other parts of the organization, law enforcement, and other external CSIRTs, security experts, and involved sites. They also will develop the main mitigation strategies and response solutions for any incident activity and distribute this to relevant system, network, and security administrators in the field. They can also update higher level management and any other divisional or functional managers as needed.

For this coordination effort to work effectively, the CSIRT must have points of notification already established across the enterprise for notifying others about incident activity. An established relationship with the IT department and organizational system, network, and security administrators is needed.

Vulnerability and Artifact Response Coordination

A centralized CSIRT is better positioned than a security or distributed team to perform effective vulnerability and artifact response coordination, provided the necessary expertise exists in the team. With dedicated resources, the team can provide comprehensive tracking, recording, and dissemination of information to the enterprise. By consolidating the information collected, the team is better able to identify similar attacks, artifacts, exploits, trends, and patterns. Potential new threats to the enterprise can also be identified. In this centralized model, it is important that the team have expertise or familiarity with all platforms and operating systems used in the organization. If this is not possible, mechanisms need to exist for the CSIRT to call upon platform specialists in other parts of the enterprise or third party experts as needed.

Based on the results of the analysis of any vulnerability or artifact information, the CSIRT coordinates the release of remediation, detection, and recovery steps throughout the enterprise as required.

Even with a centralized CSIRT, many teams find they do not have the skills or expertise to be able to provide this vulnerability and artifact coordination service effectively, so they depend on other CSIRTs to provide analysis and recommendations to the community (e.g., vendor sites, members of FIRST, computer security experts, the CERT/CC, or other CSIRTs). In this case, the CSIRT would be a point of contact for receiving this information from other experts and disseminating it as appropriate throughout the enterprise.

Announcements

The centralized team is in a position to be a good point of contact for all incoming information from external and internal sources regarding incident activity, vulnerabilities, and intruder trends. As part of its centralized function it can review and filter all incoming information and pass it on to various parts of the organization. For this service to work properly, established channels and mechanisms for communicating information to the rest of the constituency must be in place and understood by the recipients. Established document types and distribution procedures should also be in place. Announcements might be about intruder trends noted in the general Internet community but not yet affecting the constituency, vulnerabilities that have been discovered, or new incident information that may have an impact on the enterprise. Mechanisms for disseminating announcements may include mail distribution lists, advisory mailing lists, CSIRT web page posts, or even recorded messages in phone systems.

Technology Watch

Having a dedicated staff in the centralized model means there will probably be sufficient resources to provide a technology watch service.

In this model, this service can be delivered in one of two ways. Either one or two staff can be assigned to perform this service on a full-time basis as one of their primary job functions or each member of the team can be assigned a particular technology area or platform to monitor.

If multiple assignments are made across the team, either someone will need to be assigned to consolidate the information or each person will need to send out their own information. Any information is then made available to the rest of the CSIRT staff via the secured intranet or extranet.

Security-related information that affects the organization can be posted to a mailing list or an intranet discussion site as a means of keeping network, system, and security administrators up to date. This notification can also be used to raise the level of security awareness for all members of the enterprise. Such an information distribution site can provide educational benefits by allowing people to post questions that can be answered by the CSIRT staff if time permits.

Security-Related Information Dissemination

Having a dedicated team allows the centralized CSIRT to also focus on providing security-related information to the rest of the organization.

The CSIRT can establish a centralized web site (and FTP site, if appropriate) to provide organization-wide access to appropriate security-related information. They can also use these sites to disseminate information from other external sources that has been tailored to the needs of the constituency in regard to supported technologies and software. Information can also be distributed via newsletters and mailing lists.

Information disseminated includes current activity reports, threat trends and patterns, security awareness tutorials, incident reporting forms and guidelines, current updates on CSIRT developments, and any special security-related information on various applications, protocols, and security or attack tools.

If the CSIRT web and FTP sites are not maintained by the team but by other parts of the IT group, then it will be important for the CSIRT to work closely with the administrators to ensure the server is adequately protected and that information is updated in a timely manner.

Depending on its resources, if the centralized CSIRT is international this service might also include translation of security information into other languages.

6.5.2 Additional Services

In addition to its core services, a centralized CSIRT may choose to offer other services as identified or required by the constituency. The following services are those most likely to be provided.

Incident Response On Site

In a small organization, the centralized CSIRT can be tasked with performing response and recovery steps themselves, provided the team members have the required expertise.

This is more problematic in a large, distributed organization. The problems result from the time and resources needed to send a CSIRT staff member to the affected location if they are not in the same building or geographical location. If staff are away from the centralized team, this may also affect the overall performance of the team in providing services at the central site.

For this type of service to work effectively, the centralized team will need well-established relationships with the system, network, and security administrators throughout the enterprise. Agreements that the CSIRT will handle the recovery and response steps will need to be made with any relevant divisions or business units, as well as with the IT department.

Vulnerability and Artifact Analysis

If the centralized team has staff dedicated to CSIRT work, they may have the resources and expertise to engage in technical vulnerability and artifact analysis.

If analysis is not done, information about vulnerabilities and artifacts is obtained from other entities such as other external CSIRTs and security experts, as described in "Vulnerability and Artifact Response Coordination" in Section 5.5.1.

However, for the centralized team to be able to gauge the impact and threat of a particular vulnerability or artifact across their infrastructure, they may need to rely on the expertise of the operational staff that run the various parts of the infrastructure and the business managers who are responsible for each area.

Security Audits or Assessments

With its technical expertise and experience handling new vulnerabilities, real incidents, and artifacts, the centralized members of the CSIRT could participate with an audit or assessment team in the provision of this service, or provide input into the development of compliance criteria and requirements.

The centralized team can also provide the lead in coordinating and maintaining any proactive vulnerability scanning or penetration testing that may occur.

Configuration and Maintenance of Security Tools, Applications and Infrastructures

Although it is possible for the staff of a centralized team to perform configuration and maintenance of security tools, applications, and infrastructures, that is not usually one of their primary functions. However, for some team structures, the CSIRT staff may indeed maintain border firewalls, do network monitoring, and also recommend security configurations for various systems and services on the network infrastructure. If such tasks are performed, the CSIRT staff will need to have a good understanding of the mission and function of all critical infrastructure components and their relationship to each other.

The system and network components configured and maintained can include firewalls, VPNs, IDS, and even virus scanners. Work may also involve user account and password management or the review of network, system, security, and accounting logs.

Development of Security Tools

If the centralized team has dedicated resources, these team members may develop extensive expertise related to programming and software development. In such cases members of a centralized team might develop tailored tools to provide workarounds or temporary fixes to help resolve situations in which no patch or mitigation strategy is available. Delivery of such a service will depend on the expertise of the team members and the priority of other duties and functions.

Intrusion Detection Services

The centralized model is suited for having the CSIRT have the overall authority for reviewing and summarizing intrusion detection reports. Staff can develop the necessary procedures and guidelines based on past experience that can be used at the divisional level for reporting intrusions. The CSIRT can be the focal point for providing guidance in determining normal and abnormal network behavior and identifying appropriate response mechanisms and processes.

This service can be provided in one of two ways. In the first, the centralized team is responsible for maintaining and monitoring all intrusion detection systems within the enterprise. In the second, rather than performing the monitoring themselves, the CSIRT acts as a central coordinating site for the analysis of abnormal activity reported from the field. In this second model, the maintenance and monitoring of intrusion detection systems is done at the local level by each site or division (depending on the organizational structure), and all alerts or abnormal activity are reported, on some prescribed basis, to the centralized CSIRT for review and analysis. This enables the centralized team to look for trends, patterns, and correlations regarding incident activity across the enterprise.

All involved personnel need specialized IDS training. Regardless of the way the data is received, data reduction and analysis tools and scripts will be needed to manage and review the logs and information received.

6.5.3 Impact on Security Quality Management

By having a dedicated CSIRT, this model allows for the centralization of various incident handling and data analysis functions. This model establishes the CSIRT as the central point for the collection and dissemination of information related to incident activity, reported vulnerabilities, and identified artifacts. This information is used to provide a broad picture of the security of systems and networks within the enterprise. The information gathered and analyzed can be used by the CSIRT to develop materials and guidelines to assist system, network, and security administrators in providing support to their divisions and to the organization in general. Such materials can include self-assessments and checklists to help system, network, and security administrators secure systems before they are placed in production environments. These types of materials can also be used to evaluate and troubleshoot existing systems. Other materials that can be developed include security-awareness briefs and security policies and procedures for the organizational infrastructure. These materials can be used in a proactive manner to improve the security of all organizational divisions. Having such materials provides a consistent set of procedures to follow within the enterprise, including incident reporting and response procedures.

The centralized CSIRT is also responsible for working with human resources (or a similar department) to identify the needed training for staff throughout the enterprise. The CSIRT bases its input on the common types of activity and tools that are seen or used by the constituency. A security curriculum is developed that is geared to the functional responsibility of the CSIRT staff and the constituency it serves. The team develops presentations and user awareness campaigns and offers periodic "refresher" sessions. Members of the dedicated team may be assigned to visit organizational site locations to provide briefings or security awareness training. CSIRT staff can also provide instruction on security issues, tools, and recovery techniques. The CSIRT can also develop a web presence to provide relevant information to the organization, such as FAQs, security information, newsletters, policies, procedures, and guidelines.

Incident and vulnerability trends, knowledge about weaknesses in the enterprise and needed security precautions, as well as other information gathered by the CSIRT can provide input into many security quality management services, including the provision of audits and assessments, business continuity planning, and disaster recovery planning.

With a dedicated, centralized CSIRT there may be more time and opportunity available for CSIRT staff to devote to product evaluation or security consulting. The CSIRT, due to its position in the organization, should be heavily involved in the development of enterprise-wide se-

curity policies. What the team is actually able to do will depend on its size, mission, and workload.

6.6 Resources

The following staff, equipment, and infrastructure resources should be considered when implementing a centralized CSIRT model.

6.6.1 Staff

A centralized team can dedicate up to 100% of their effort to provide CSIRT services. The CSIRT is centrally located and coordinates activities across the enterprise. Its staff will most likely contain the following individuals:

- one manager (with a designated backup)

- one administrative support person

- technical staff – The number of technical analysts will depend on the size of the CSIRT constituency, available resources, and services offered. Also, if the CSIRT provides 24x7x365 coverage, then more staff may be needed.

In some organizations staffing levels may be from 1 to 4 and in others from 5 to 10 or more. Some organizations may have designated positions for the CSIRT but fill them with a number of rotating staff. For example, 1 or 2 staff may be assigned incident handling duties for a week. The following week different staff members perform the work for this position. Some teams in Europe call this a "Rota" model.[45]

If resources permit, the centralized team may also include

- one system administrator to provide infrastructure support for the CSIRT equipment (this can also be a shared position with another department)

- one or more triage staff. If the CSIRT provides a hotline or help desk, the person in this position can also perform that function. (These staff should have a mix of administrator/junior system administrator skills.)

There may be additional adjunct staff who may work with the CSIRT on an as-needed basis from other areas of the organization, including

- technical writers

- trainers/instructors

---

[45] More information about this model can be found in Section 4.2 of the JANET document *Effective Incident Response* available at <http://www.ja.net./documents/incident-response.pdf>.

- public affairs staff

- web developers

- human resource representatives

- legal counsel

- investigators

- other technical experts as required by the systems and applications supported by the enterprise. (These could include database administrators, application developers, managers, platform specialists, network administrators, auditors, and risk management personnel. They may work as extended members of the team.)

Having an established and effective communications plan with these additional areas is crucial to the success of the incident handling functions.

The total number of staff needed depends on the number of services provided, the size of the constituency, and the number of reports received by the CSIRT.

The CSIRT staff can call upon identified organizational contacts and/or system, network, and security administrators to respond to security events at the local level, or they may go to the local site to provide hands-on assistance (if this is part of the service the team provides). The staff will need to coordinate with any IT staff responsible for security and perimeter defenses.

With the centralized model, incident handling activities are coordinated and managed by the CSIRT. If the requisite skills are not resident in the CSIRT, the team may be able to negotiate with other local system administrators and existing security teams for assistance as needed. If there is an enterprise-wide help desk function, the CSIRT needs to coordinate with that staff.

6.6.2 Equipment

Equipment is needed to support the centralized CSIRT staff. This includes (but is not limited to) the following:

- office space and furniture (desks, copier, supplies, etc.)

- computer equipment for day-to-day operations and activities

- non-production test lab facilities

- travel and home equipment (for remote access, training, and on-site visits)

- telephones (secure telephones, fax, cellular, pagers)

Where required, CSIRT staff negotiate for the use of other equipment for testing (e.g., in existing test labs). If the CSIRT is unable to acquire the use of needed equipment they may have to

purchase this equipment at additional cost. It is also possible for the CSIRT to build a collaborative, trusted relationship with other external agencies and to call upon these other expert resources for assistance in analysis and/or testing.

6.6.3 Infrastructure

The infrastructure must provide a secure environment for the CSIRT's day-to-day operations. It should include (but is not limited to) the following:

- physical security

- protected power sources and generator (if appropriate)

- a firewall or separate network to isolate the CSIRT network from the rest of the organization

- network and host security

- secure intranet

- a robust and secure tracking system

- a secure repository for incident, vulnerability, and artifact data

- secure communications support (email, phones, videoconference, etc.)

- web services

- encryption technologies

- virus protection and scanning software

- secure backups and storage of CSIRT data

6.7 Summary

This model has staff dedicated to CSIRT work located in one central site, reporting to a high-level manager, such as a CIO, CSO, or CRO. Team members are usually assigned 100% to CSIRT work; some organizations, however, may be able to use part-time staff. In some situations there may be staff resource sharing, as appropriate, for assistance in areas such as infrastructure support, technical writing, investigations, and media relations.

6.7.1 Impact on Constituency

This centralized model provides the organization with a clear mechanism for proactively managing its computer security risks and provides a broader understanding of the security threats and activity affecting the constituency. The dedicated team provides resources to expand the focus of the CSIRT beyond reactive services by providing more time to devote to proactive and security quality management services. The organization can now analyze potential threats

and risks and determine the appropriate levels of prevention and mitigation necessary to provide adequate levels of security.

The major impact to the constituency is that now it must interface with the CSIRT. This means that the constituency must understand the function and purpose of the CSIRT. It must be trained in how and when to contact the CSIRT. Divisions that previously handled their own incident and vulnerability response must now learn to work closely with the CSIRT. New policies and procedures, organizational processes, and communications mechanisms must be developed. The CSIRT work and functions must be integrated into the existing enterprise.

In turn, the CSIRT must take the time and effort to understand not only the enterprise infrastructure but also the business needs and priorities of each part of the organization. This will require establishing good channels of communication between the CSIRT and other parts of the organization and a methodology for interacting with other business sectors to get their input and expertise during incidents that affect their systems and networks.

The CSIRT must be included in all long-term strategic planning regarding not only infrastructure support but also the implementation of new business services. This will help them to understand the service from its beginning so that they can provide insight into any security problems or issues that must be addressed, and also so they can understand the priority and function of this service so that they can provide the best response possible.

The CSIRT should also be involved in any change management or configuration management systems or communications channels that exist in the organization. The CSIRT needs to be aware of changes in the infrastructure and also needs to understand what type of configuration defenses are in place. Based on their understanding of current security problems and intruder trends, the CSIRT can also provide input into best practices for configuring systems in a secure fashion.

6.7.2 Constraints

Constraints for the effective operation of a centralized team include the large number and diverse platforms used by the organization, the organization's size, and the geographic locations of the divisions and sections. Such variables might make it difficult for one centralized group of security experts to handle all incoming incidents, especially if on-site support is part of the service.

If the parent organization or constituency is small, there may not be any problems or constraints in providing these services. At the same time, there may be difficulty in having enough funding, expertise, and resources to devote to a CSIRT. In that case, the team itself may be small or composed of staff who only work as a CSIRT member on a part-time basis.

6.7.3 Strengths and Weaknesses of the Model

In this centralized model, the CSIRT is composed of dedicated computer security professionals. This structure allows for an infrastructure dedicated to incident handling. It lends itself to formalized procedures, the creation and maintenance of a central repository of incident data, and the expertise to analyze the data for maximum advantage. This structure seems to provide the best support for developing and retaining the specialized expertise that many of the sophisticated CSIRT services require.

This model provides a very stable structure for building a CSIRT. This makes the organization's incident handling capability manageable and predictable.

The centralized model requires that a new specialized unit be created, staffed, and integrated into the organization's operations.

The main weakness of this model is that now the incident handling capability is separate and distinct from other operational units. The CSIRT has specialized security expertise but may lack operational knowledge. The operational units may assume that the CSIRT will handle all computer security events and therefore not be concerned about such issues themselves. The CSIRT may become disconnected from the operating units, making it difficult for the dedicated team to integrate and coordinate across a large enterprise. Also, having a centralized team may concentrate incident handling knowledge and skills in a small number of staff. When this staff leaves, there may be a more disproportionate loss of organizational knowledge, from which the CSIRT may not easily recover. In a centralized model, therefore, the cross-training and mentoring of staff and designated backups for each staff member is vitally important.

It is also vitally important that the roles and responsibilities and interactions of staff across the organization are clearly defined and understood.

The strengths and weaknesses of this model include the following:

- Strengths
  - Ideally, there is a focused, dedicated team that does not have to divide its time between CSIRT work and other responsibilities.
  - The CSIRT provides staff trained in computer security incident response and recovery.
  - The CSIRT provides a central responsibility for synthesizing and analyzing information to determine trends and patterns for the entire enterprise. This facilitates the quick identification of targeted attacks.
  - There is a central repository for storing incident, vulnerability, and artifact data and related materials.

- The CSIRT is able to provide valuable information to the constituency (documents, checklists, best practices, etc.).
- The CSIRT is able to build a comprehensive knowledgebase of incident and vulnerability reports, analysis, and response strategies.
- It is easier to build and maintain a strong team atmosphere.

- Weaknesses
  - It may be more difficult to coordinate with any geographic and divisional sites, if they exist.
  - Without strong management support, the team may seem isolated from the rest of the organization.
  - The organization needs to fill a number of new positions and purchase additional equipment and furnishings.
  - It can be difficult to determine the correct size of the team.
  - It can be difficult to obtain sustained funding of the CSIRT.
  - Depending on where the CSIRT is organizationally located, it can be difficult to get buy-in from other divisions to follow the recommendations of the CSIRT.
  - It is difficult to cover all the areas of expertise necessary; the CSIRT may not have enough staff to handle all supported platforms.
  - It is difficult to ensure that all divisions act on recommendations in a timely, appropriate manner.
  - Information may have to flow through several hierarchical levels to reach appropriate individuals who are ultimately responsible for implementing repairs, causing delays in response and recovery.
  - Incident handling knowledge may be concentrated in a few staff members, resulting in a loss of organizational knowledge when staff leave.
  - It is difficult to provide a team with up-to-date operational knowledge of the enterprise. The team must develop, understand, and maintain a picture of the organization's critical infrastructure.

7 Combined Distributed and Centralized CSIRT

7.1 Overview

In this model a dedicated, centralized CSIRT is established that interacts with team members who are distributed throughout the organization in various geographic sites and divisions. The centralized team provides high-level analysis and recommends recovery and mitigation strategies. It also provides incident, vulnerability, and artifact response support for the distributed team members and other parts of the enterprise. The distributed team members at each site implement the strategies and provide expertise in their areas of responsibility. This model is referred to as the "combined CSIRT" throughout the rest of this document.

This model maximizes the utilization of existing staff in strategic locations throughout the organization with the centrally located coordinating capability of the dedicated team to provide a broader understanding of the security threats and activity affecting the constituency. It has management support in assigning needed resources during times of crisis.

It builds on the infrastructure and expertise in the local areas where the distributed team members facilitate incident analysis and response (working with others in the organization—system, network, and security administrators, software developers, LAN/WAN managers, etc.—who are not part of the CSIRT). The CSIRT responds to reports of abnormal activity or other incident reports, participates in incident and vulnerability analyses, lends expertise in testing or assessing the security of the enterprise, and plays a proactive role in promulgating computer security awareness and training throughout the organization.

The model provides a centralized team that can collect information from a wide variety of constituent sources and quickly synthesize and disseminate it across the enterprise.

The combined team works best if it has full authority to analyze activity and shared authority to respond to incident activity as it occurs. No enterprise-wide action is taken or recommended without the approval of the CSIRT manager and possibly upper management such as a CIO, CSO, or CRO. The team also has the authority to enforce recovery and mitigation strategies with the approval and consent of the management. Divisional and functional unit managers are

notified of any action to be taken in their areas and are involved in the decision-making process to determine how to implement a response.

The team has the authority to release organization-wide advisories and other documents, including best practices, response and recovery steps, and security updates. The team can also be responsible for reviewing and analyzing all IDS or other network, system, or application logs. It should be pointed out that in some commercial organizations the CSIRT may have to play a subordinate role to a crisis management "team" during an incident. This is a team that is pulled together by management to handle any type of emergency situation. If this is the case, again, it will be important to clearly delineate roles, responsibilities, communication paths, and authority.

7.2 Supported Constituencies

This model works best for very large distributed organizations or constituencies. Although conceptually this model will work in a small organization, it is probably not necessary, and a centralized model would work better.

This combined model may have the same problems as the centralized CSIRT if the constituency is a large organization with multiple affiliate or subsidiary companies or groups.[46] In this case, although seen as part of the same parent entity, each affiliate or subsidiary might have its own management structure, policies, procedures, and authority, or even its own internal CSIRT. This may cause problems in how much authority the combined CSIRT has over the systems, networks, and incident handling efforts in the affiliates/subsidiaries and may also cause problems in effecting a consistent level of response across these disparate units. Although a combined CSIRT can work in this organizational situation, a coordinating model may work better (see Section 8).

7.3 Organizational Structure

The combined team merges the characteristics and structure of the distributed CSIRT model and the centralized CSIRT model.

The combined team has a central location close to and reports to a top-level manager (such as a CIO, CSO, or CRO). The manager or designee represents the CSIRT in any organizational activities and groups related to computer security, internally as well as externally. There is generally a small, centralized core staff and then the distributed members are scattered throughout the organization.

---

[46] As described in Section 6.2, "Supported Constituencies," for an internal centralized CSIRT.

There are a multitude of ways that a combined CSIRT can be configured regarding work assignments.

- One approach is to have the centralized team perform all triage and analysis work and task the distributed team to implement the response steps or procedures at their specific sites.

- Another approach is to have the centralized team just receive incident reports and then assign the actual analysis and response to the appropriate distributed team members based on functional expertise and geographic location.

- Still another option is to outsource all or part of the work of the centralized team to a third party contractor, which is managed by the CSIRT. The contracting organization may have staff on site as extended members of the CSIRT and may work with other distributed team members in the field.

It is possible in this model to have smaller teams of centralized and distributed team members pulled together to handle a specific incident. This can work well in organizations with a relatively small number of incidents. In larger organizations, a more formalized structure may be needed. Another approach to using the distributed staff is to identify individuals throughout the organization with defined subject matter expertise. The centralized team can then perform the majority of the incident handling tasks but call on these subject matter experts (SMEs) as needed.

Distributed team members can either be dedicated to CSIRT operations on a full-time basis or they can work part-time for the CSIRT in addition to their normal responsibilities. If the distributed members only perform CSIRT work part-time, then established agreements are necessary to outline when and how the distributed team members will work with the CSIRT. The distributed team member must be able to devote time to incident handling activities as required by the needs of the CSIRT. It is not recommended to have centralized staff members working on a part-time basis. However, in some instances, due to budget constraints, it may not be possible to have all full-time centralized team members. Instead there may be a core set of assigned staff who share responsibility for CSIRT functions. So there is always someone on the centralized team, but each staff member rotates on and off the team periodically.

All team members will need to use secure email or a secure intranet or extranet to communicate with members of the distributed team in the various operational units across the organization.

As part of a mentoring process, distributed team members can spend a period of time working in the central office to more fully understand the CSIRT services and operational framework, policies, procedures, and processes. This is also a way to develop personal relationships between central and distributed team members. In correlation with this, members of the centralized staff can spend some time at the distributed sites to better understand their working environment and computer security needs.

7.4 Triage

In the combined model, triage can be offered through two different structures. In the first, all reports and requests come into the central CSIRT office and are categorized, sorted, and prioritized there. In the second, reports come into the distributed sites, where initial triage is done and activity, events, or requests that cannot be handled by the distributed team are passed to the central office staff. In either case the centralized staff synthesize and track all reports.

No matter what structure is used to deliver the triage service, centralized incident and vulnerability tracking databases must be available and accessible by all members of the combined CSIRT, centralized and distributed alike. The team members access the central database to

- report problems (open reports or incidents)

- check on status

- update/close/reopen reports

- search for similar activity reports to identify solutions

Although accessible by all members of the CSIRT staff, these databases are owned and maintained by the central office.

As in the centralized and distributed models, well-defined policies and procedures for reporting incidents are available to constituents, and constituents are encouraged to report activity without fear of retribution.

7.5 Available Services

The following sections describe how CSIRT services might be provided in a combined CSIRT. It is recognized that every team is different, so these are general descriptions based on observations of and discussions with other teams. The method in which the service is delivered assumes a certain level of infrastructure, staff, and equipment, which are discussed in further sections.

7.5.1 Core Services

The core services characterizing this model do not differ significantly from those listed earlier in Section 5.5.1 (core services for an internal distributed CSIRT) or 6.5.1 (core services for a centralized CSIRT). The basic difference is in the approaches by which the services are offered and managed.

Alerts and Warnings

In a combined model, all alerts and warnings coming into the CSIRT or parent organization from other security experts, vendors, or CSIRTs are received by the centralized team component of the CSIRT. Information is usually received through some designated point of contact such as a CSIRT phone number or email alias. From there the alerts and warnings are disseminated to various points of contact throughout the organization, which are usually the distributed members of the team but which also might include system and network administrators, business managers, or security teams at distributed sites.

General alerts and warnings that affect all members of the constituency are sent to a predetermined mailing list by the centralized team. In this way a common message with a consistent set of steps to prevent or respond to any activity or security incidents can be sent throughout the organization. For this service to work efficiently there must be an up-to-date list of people and units to notify. This service fits well in a combined model.

If alerts, warnings, or advisories for the CSIRT's constituency need to be developed, these are assigned by the CSIRT manager to a member of the centralized team. The assigned staff can enlist the help of others in the organization or other members of the distributed team who have expertise that might be needed. They may also want to work with a technical writer to produce the final versions. If a technical writer is not on staff as part of the CSIRT, it may be possible to use staff with the needed skills from the constituency or parent organization. Whatever arrangement is used to obtain technical writing assistance, it should be established in advance, so that the technical writer can be called as needed.

Incident Analysis

The combined CSIRT incorporates a full-time, dedicated, centralized team with a distributed team that draws on existing expertise across the enterprise. Like the centralized CSIRT, the combined CSIRT has the resources to coordinate incident analysis at a higher level, to understand what is occurring across the enterprise, and to work with the local administrators to implement incident response actions as required.

The combined team uses resources throughout the enterprise (e.g., software testing labs, specific platform or software expertise) to conduct analysis. Tasks such as reviewing logs or monitoring intrusion detection systems can be assigned to distributed team members or handled by the central team. If handled at the local level, the results of these reviews are then shared with the centralized team members, who consolidate the data to determine patterns and trends across the organization and identify any additional work or follow-up actions to be passed back to the distributed team members for implementation.

Results of analysis are archived and accessible in a CSIRT database for daily operations and for future reference by all team members.

Incident Response Support

Combined CSIRT members work together to develop materials and disseminate information to the rest of the enterprise. For example, once solutions are identified and distributed by the centralized team, the distributed team members communicate the appropriate information to the local system, network, and security administrators and provide guidance and assistance on implementing recovery procedures for the reported activity.

Part of this service can be to provide direct assistance via telephone or email to the distributed members. It can also include providing this support to system, network, and security administrators across the enterprise. The amount of this work done will depend on the depth and breadth of services provided by the CSIRT and the size and expertise of the staff in both the central and distributed parts of the team.

CSIRT staff develop and document mitigation and recovery strategies to address the immediate threat for distribution to the rest of the organization as necessary. This notification can be achieved through secure mailing list aliases, secure web intranet or extranet servers, or even via phone or fax. Timely information that is important for all organizational staff to receive can be distributed via internal employee mailing lists if necessary.

One of the strengths of building a robust combined CSIRT is that the centralized and distributed members of the entire team all have a coordinated approach to handling CSIRT activities and they work in concert to ensure that remediation and response is handled appropriately. So, in those cases where immediate action must be taken, the distributed members have the requisite authority and understanding of what to do to activate responses independent of direction from the centralized part of the team. That is, they can undertake response or repair systems without receiving information, alerts, advisories, or guidance from the centralized team. However, as the distributed teams initiate such responses, they also communicate their actions with the centralized team to ensure the overall coordination of any enterprise-wide efforts.

Incident Response Coordination

This service is mainly provided by the centralized staff of the CSIRT. As the focal point for incident analysis and response, they coordinate the activities of the distributed team members to respond to enterprise-wide events and activity. The distributed team members, in turn, confirm that the local administrators have implemented the appropriate actions and relay this information back to the centralized team.

The centralized staff also acts as the liaison to other external CSIRTs, security experts, and sites that the CSIRT might need to contact or collaborate with. The CSIRT is the main point of contact for all incident and vulnerability work. They are also the liaison with legal counsel,

CMU/SEI-2003-HB-001

human resources, upper management, and any other organizational group dealing with security issues.

Vulnerability and Artifact Response Coordination

Just like the centralized team, a combined CSIRT is better positioned than a security or distributed team to perform effective vulnerability and artifact response coordination, provided the necessary expertise exists in the team. With dedicated resources, the centralized team component of the CSIRT can provide comprehensive tracking, recording, and dissemination of information to the enterprise. By consolidating the information collected, the team is better able to identify similar attacks, artifacts, exploits, trends, and patterns. Potential new threats to the enterprise can also be identified. In this model, it is important that the team have expertise or familiarity with all platforms and operating systems used in the organization. If this does not exist within the centralized team component, then there must be mechanisms in place to collaborate with the distributed team members or other organizational experts who can provide the required knowledge.

Based on the results of the analysis of any vulnerability or artifact information, the CSIRT coordinates the release of remediation, detection, and recovery steps throughout the enterprise as required.

Even with centralized CSIRT component, many teams find they do not have the skills, expertise, or time to be able to provide this vulnerability and artifact coordination service effectively, so they depend on other CSIRTs to provide analysis and recommendations to the community (e.g., vendor sites, members of FIRST, computer security experts, the CERT/CC, or other CSIRTs). In this case, the centralized component of the CSIRT would be a point of contact for receiving this information from other experts and disseminating it as appropriate throughout the enterprise. This does not preclude distributed members from receiving information from security mailing lists and advisory lists. Anything the distributed members receive from external sources should be shared with the centralized team to ensure that everyone has seen the information.

Announcements

The centralized component of the CSIRT is in a position to be a good point of contact for all incoming information from external and internal sources regarding incident activity, vulnerabilities, and intruder trends. As part of the centralized function the team can review and filter all incoming information and pass it on to the distributed team members and to any other designated parts of the organization.

For this service to work properly established channels and mechanisms for communicating information to the rest of the constituency must be in place and understood by the recipients. Established document types and distribution procedures should also be in place. Announcements might be about intruder trends noted in the general Internet community but not yet af-

fecting the constituency, vulnerabilities that have been discovered, or new incident information that may have an impact on the enterprise. Mechanisms for disseminating announcements may include mail distribution lists, advisory mailing lists, CSIRT web page posts, or even recorded messages in phone systems.

Technology Watch

Having a dedicated staff in the centralized component of the combined team model means there will probably be sufficient resources to provide a technology watch service. This service could be offered in a number of ways. The centralized staff could take all responsibility for doing the research and synthesis of this information, or assignments could be made to members of the distributed team, based on their expertise and interest.

No matter who collects and researches the information, the centralized team consolidates the information and disseminates it to the rest of the combined team and to any other appropriate members of the enterprise. Consolidated information can include current threats and trends, new technologies, new attacks, new tools, or even legal issues that may potentially affect the organizational operations of the enterprise or the CSIRT. The distributed members of the team can then pass this information along to those at their site who they feel should see it.

Security-related information that affects the organization can be posted to a mailing list or an intranet discussion site as a means of keeping network, system, and security administrators up to date. This notification can also be used to raise the level of security awareness for all members of the enterprise. Such an information distribution site can provide educational benefits by allowing people to post questions that can be answered by the CSIRT staff if time permits.

Security-Related Information Dissemination

In the combined model, the centralized team component allows the CSIRT to focus on providing security-related information to the rest of the organization.

The CSIRT can establish a centralized web site (and FTP site, if appropriate) to provide organization-wide access to appropriate security-related information. They can also use these sites to disseminate information from other external sources that has been tailored to the needs of the constituency in regard to supported technologies and software. Information can also be distributed via newsletters and mailing lists. Special communication plans between the centralized and the distributed team members need to be in place along with a supporting infrastructure so that the two areas can communicate in a secure fashion when needed, and can quickly get a hold of each other. This may mean special mailing lists, phone trees, or other communication channels need to be established and kept up to date.

Information disseminated includes current activity reports, threat trends and patterns, security awareness tutorials, incident reporting forms and guidelines, current updates on CSIRT devel-

opments, and any special security-related information on various applications, protocols, and security or attack tools.

·If the CSIRT web and FTP sites are not maintained by the team but by other parts of the IT group, then it will be important for the CSIRT to work closely with the administrators to ensure the server is adequately protected and that information is updated in a timely manner.

7.5.2 Additional Services

In addition to its core services, a combined CSIRT may choose to offer other services. The following services are those most likely to be provided.

Incident Response On Site

On-site assistance is possible in this model when supported by the distributed team members. While the centralized team continues to provide CSIRT services such as incident response support, the knowledge and expertise of distributed team members can substantially increase the ability of the organization to handle incidents effectively and efficiently at the local levels.

If this service is offered it will most likely be done by the distributed team members who know the systems and networks at the remote sites. For this to work effectively they must have good relationships with the existing system, network, or security administrators at the sites. In most cases, they are probably system, network, or security administrators themselves.

Intrusion Detection Services

In this model the overall authority for reviewing and summarizing intrusion detection reports can be given to the centralized component of the combined CSIRT, if appropriate. This gives a dedicated and focused group the responsibility for this task. Distributed team members can be called upon to provide more in-depth operational and business knowledge and assistance for the analysis as required. If other parts of the organization provide intrusion detection services, the CSIRT should establish agreements and channels of communication for getting information from or access to their logs when necessary.

For the delivery of this service the central CSIRT can be responsible for monitoring the IDS for the whole enterprise. Alternatively, the initial review of the logs can be done by the distributed team members or even other system and network administrators at the local level. Logs are still sent to the central CSIRT for further analysis, where they can be synthesized to determine if there are any patterns or trends that would indicate specific network activity that cannot easily be seen by doing a daily review at the local level.

In this combined model all involved personnel need specialized IDS training. The centralized CSIRT, with input from the distributed members, provides guidance on distinguishing normal

and abnormal network behavior and identifies appropriate response mechanisms and processes for any abnormal activity seen.

Vulnerability and Artifact Analysis

If the centralized component of the combined team has staff dedicated to CSIRT work, they may have the resources and expertise to engage in technical vulnerability and artifact analysis.

If analysis is not done, information about vulnerabilities and artifacts is obtained from other entities such as other external CSIRTs and security experts, as described in "Vulnerability and Artifact Response Coordination" in Section 5.5.1.

However, for the centralized team component of the CSIRT to be able to gauge the impact and threat of a particular vulnerability or artifact across their infrastructure, they may need to rely on the expertise of the operational staff that run the various parts of the infrastructure and the business managers who are responsible for each area.

Security Audits or Assessments

With its technical expertise and experience handling new vulnerabilities, real incidents, and artifacts, the centralized component of the combined CSIRT could participate with an audit or assessment team in the provision of this service, or provide input into the development of compliance criteria and requirements.

The centralized team can also provide the lead in coordinating and maintaining any proactive vulnerability scanning or penetration testing that may occur. However, various members of the distributed team could also provide part of these services for their particular section of the organization and report the results back to the centralized component.

Configuration and Maintenance of Security Tools, Applications and Infrastructures

Configuration and maintenance of security tools, applications, and infrastructures could be part of the assigned tasks given to the distributed members of the combined CSIRT if this is part of their normal operational work or if they are the system and network administrators for the related parts of the infrastructure. If the distributed team members do not have technical skills, this would not be a service they would provide.

Although it is possible for the staff of the centralized team component of the combined CSIRT to perform configuration and maintenance of security tools, applications, and infrastructures, that is not usually one of their primary functions. However, for some team structures, the CSIRT staff may indeed maintain border firewalls, do network monitoring, and also recommend security configurations for various systems and services on the network infrastructure. If

such tasks are performed, the CSIRT staff will need to have a good understanding of the mission and function of all critical infrastructure components and their relationship to each other.

The system and network components configured and maintained can include firewalls, VPNs, IDS, and even virus scanners. Work may also involve user account and password management or the review of network, system, security, and accounting logs.

Development of Security Tools

If the centralized component of the combined team has dedicated resources, these team members may develop extensive expertise related to programming and software development. In such cases members of a centralized team might develop tailored tools to provide workarounds or temporary fixes to help resolve situations in which no patch or mitigation strategy is available. Delivery of such a service will depend on the expertise of the team members and the priority of other duties and functions. It is also possible that various members of the distributed team, if they have a background or operational knowledge as system and network administrators, may also be able to develop such tools for use in their part of the infrastructure.

7.5.3 Impact on Security Quality Management

By having a distributed team working in conjunction with a centralized team, a framework for incident management is established that provides a dedicated staff with skills in incident analysis and response and distributed members with expertise in the various business systems scattered throughout the enterprise.

The centralized team can focus on analyzing patterns of activity across the enterprise. They can use this information and the knowledge gained by doing incident and vulnerability handling to provide recommendations on defensive strategies to implement to protect the critical assets of their constituency. They can use this information to create configuration guidelines, security awareness briefings, technical reports, and training.

The distributed CSIRT members have a connection to the various sites within the enterprise. They should have established working relationships with business managers and IT staff at these sites, so that they can implement the recommendations and strategies provided by the centralized CSIRT staff. Their work at the sites provides the CSIRT with an operational understanding of the enterprise that a centralized staff by itself would not have.

The CSIRT manager makes assignments (such as authoring best practice documents and developing bulletins, alerts, and checklists) to the appropriate centralized and distributed team members who have experience in the related platform or system. Short-lived, ad hoc teams may come together to develop particular materials, providing more opportunity for the distributed and centralized team members to work together and share information.

This combined team creates a two-way line of communication between the distributed sites and the centralized component of the CSIRT. Staff can use this information flow to get information into the team and to pass security awareness training, response steps, or general knowledge back to the local administrators.

The centralized team, with input from the distributed team, works with human resources (or a similar department) to identify needed computer security training for the organization. The CSIRT bases its input on the common types of activity that are seen and the tools used by the constituency. A security curriculum is developed that is geared to the functional responsibility of the CSIRT constituency and staff.

Members from both the centralized and distributed teams can be assigned to visit various organizational site locations to provide briefings, security awareness training, and instruction on security issues, tools, and recovery techniques. Distributed team members can rotate through periodic assignments in the centralized team office to broaden their security training and help them better interact with the centralized team. The central staff members can also do periodic rotations at the distributed team locations to better understand their processes and needs.

Incident and vulnerability trends, knowledge about weaknesses in the enterprise and needed security precautions, and other information gathered by the CSIRT is useful in many security quality management services, including the provision of audits and assessments, business continuity planning, and disaster recovery planning.

Having a distributed team can provide the centralized team more time to devote to product evaluation or security consulting. The CSIRT, due to its position in the organization, should be heavily involved in the development of enterprise-wide security policies. Where appropriate, members of the distributed team may be pulled into security quality management initiatives and services based on their technical knowledge and operational understanding of the business functions of the enterprise.

7.6 Resources

The following staffing, equipment, and infrastructure resources should be considered when implementing a combined CSIRT model.

7.6.1 Staff

A combined CSIRT provides a centralized staff that devotes 100% of their time to incident response services. The distributed team supplements and supports the CSIRT core activities on a full- or part-time basis.

The centralized staff contains the following individuals:

- one manager and a designated backup

- one administrative support person

- several (typically four to six) technical staff (equivalent to experienced system/network administrators or others who have experience in incident/vulnerability handling activities, preferably those who have expertise with platforms supported by the organization). The number of technical staff needed will depend on the size of the constituency and the number and level of services offered.

- one or more system administrators to provide infrastructure support and possibly platform expertise (could be shared with other departments)

- one or more hotline/help desk staff. These staff can also perform triage and can be shared with other parts of the organization such as a centralized help desk. These positions are optional.

The distributed staff is composed of

- sufficient distributed staff (number determined by parent organization) with appropriate backups identified

- adjunct staff who are part of the CSIRT on an as-needed basis (previous agreements on interactions with the CSIRT would need to be defined and agreed to by management):
  - technical writers
  - trainers/instructors
  - public affairs staff
  - legal/criminal investigators
  - other technical experts (Windows, UNIX, or mainframe experts; database administrators; managers)

The size of the distributed team is determined by the size and diversity of the organization. It can consist of 10 members or 50 or even more. It might be comprised of several smaller teams dispersed throughout the organization (e.g., geographically located or organizationally delineated) that serve a specific division, area, or set of individuals.

7.6.2 Equipment

Equipment is needed to support the centralized CSIRT staff. This includes (but is not limited to) the following:

- office space and furniture (desks, copier, supplies, etc.)

- computer equipment for day-to-day operations and activities

- non-production test lab facilities

- travel and home equipment (for remote access, training, and on-site visits)

- telephones (secure telephones, fax, cellular, pagers)

The distributed team members use computer equipment, telephones, pagers, etc. that are already part of the organization's infrastructure or that are purchased for the CSIRT's use. In either case, they need access to secure phones, email, and intranets/extranets to be able to effectively and securely correspond with the centralized team. This might be easier if the computer equipment is also fully controlled by the CSIRT.

7.6.3 Infrastructure

The infrastructure provides a secure environment for CSIRT day-to-day operations. This includes (but is not limited to) the following:

- physical security

- protected power sources and generator (if appropriate)

- a firewall or separate network to isolate the CSIRT network from the rest of the organization

- network and host security

- secure intranet

- a robust and secure tracking system (trouble ticket system, relational database, etc.)

- secured repository for storing and archiving all incident and vulnerability data

- secure communications support (email, phones, faxes, videoconference, etc.)

- web services

- encryption technologies

- virus protection and scanning software

- secure backups and storage for CSIRT data

The distributed team members will need to use some type of protected network connection such as a VPN or extranet to work collaboratively with the centralized team. In essence a separate CSIRT network is required throughout the enterprise to protect the incident and vulnerability handling information and related materials such as emails, advisories, and any other site sensitive data that the team members will access. Secure access to the central incident tracking system will be paramount for this model to work effectively.

As with the distributed model, if needed equipment cannot be borrowed or purchased, collaborative agreements can be made with other trusted experts to conduct needed analysis and testing.

7.7 Summary

In the combined CSIRT a dedicated, centralized team is augmented with distributed team members from the functional business operating units.

7.7.1 Impact on Constituency

This combined model provides the organization with a clear mechanism for proactively managing its computer security risks and provides a broader understanding of the security threats and activity affecting the constituency. The model leverages the CSIRT capabilities of the distributed team members to provide a localized view into the constituency. This increases their ability to assess the state of the enterprise very rapidly by sharing information between the distributed and centralized team members. This information allows the organization to analyze potential threats and risks across the enterprise and to determine the appropriate levels of prevention and mitigation necessary to provide adequate levels of security.

The major impact to the constituency is that now it must interface with the CSIRT. This means that the constituency must understand the function and purpose of the CSIRT. It must be trained in how and when to contact the CSIRT. Divisions that previously handled their own incident and vulnerability response must now learn to work with the CSIRT. New policies and procedures, organizational processes, and communications mechanisms must be developed. The CSIRT work and functions must be integrated into the existing enterprise. The transition to this model, however, can be facilitated by the distributed team members, who are already working at the local level and are known to the constituents.

In turn, the centralized CSIRT must take the time and effort to understand not only the enterprise infrastructure but also the business needs and priorities of each part of the organization. This will require establishing good channels of communication between the CSIRT and other parts of the organization and a methodology for interacting with other business sectors to get their input and expertise during incidents that affect their systems and networks. Again, the distributed team members can help facilitate this interaction.

The CSIRT must be included in all long-term strategic planning regarding not only infrastructure support but also the implementation of new business services. This will help them to understand the service from its beginning so that they can provide insight into any security problems or issues that must be addressed, and also so they can understand the priority and function of this service so that they can provide the best response possible.

The CSIRT should also be involved in any change management or configuration management systems or communications channels that exist in the organization. The CSIRT needs to be aware of changes in the infrastructure and also needs to understand what type of configuration defenses are in place. Based on their understanding of current security problems and intruder

trends, the CSIRT can also provide input into best practices for configuring systems in a secure fashion.

7.7.2 Constraints

The main constraints in this model are the difficulty of building and operating a dispersed team across a variety of geographical and physical locations. Other challenges include ensuring that the distributed and centralized staff work together effectively and implementing a feedback mechanism to ensure that response efforts are carried out according to the CSIRT's guidelines.

If the distributed parts of the organization are in other countries or are separate affiliated companies, there may also be difficulties in coordinating actions because of differences in policies, languages, laws, and time zones.

7.7.3 Strengths and Weaknesses of the Model

The strengths of this combined model are that it provides a CSIRT composed of a stable core of professionals along with a network of affiliated members in the operating units. The centralized members provide the stability, expertise, and permanent infrastructure, while the distributed members provide the operational knowledge and expertise, along with established connections to the business units at the local levels.

The greatest weakness to this approach is that now there are two systems to manage and coordinate. If not handled well, the result may be a disconnected centralized team along with an ineffectual distributed component.

The strengths and weaknesses of this model include the following:

- Strengths
    - CSIRT functions are performed by a focused, dedicated staff who are trained in computer security response and recovery.
    - The distributed team members in the field support the centralized team, providing expertise in the local systems and operations.
    - There is coordinated incident reporting, analysis, and response across the enterprise.
    - There is a centralized responsibility for synthesizing and analyzing information to determine trends and patterns for the entire enterprise. This provides a consolidated and comprehensive view of the vulnerabilities and incident activity across the constituency.
    - There is a central repository for incident, vulnerability, and artifact data and related information.

- The CSIRT is able to use this information to provide valuable guidance and recommendations to the constituency (advisories, alerts, warnings, technical documents, checklists, best practices, etc.).
- This model facilitates the implementation of organization-wide computer security guidelines and procedures.

- Weaknesses
    - It is difficult to coordinate with all geographic and divisional sites.
    - The centralized team may seem isolated from the rest of the organization.
    - The distributed team may believe responsibility rests with centralized members.
    - The organization may need to fill a number of new positions and purchase additional equipment.
    - It is difficult to determine the correct size of the CSIRT staff.
    - The CSIRT will need to obtain sustained funding for central and distributed team expenses.
    - Depending on the location of the centralized CSIRT in the organization, it can be difficult to get support from other divisions to follow CSIRT recommendations.
    - It is difficult to manage and coordinate coverage in all the areas of expertise necessary.
    - Finding "experts" in the organization may be cumbersome and over time there can be problems with turnover, as well as training issues.
    - It can be difficult to ensure that all divisions act on recommendations in a timely, appropriate manner.
    - Information may have to flow through division heads to be implemented, causing a delay in response and recovery time.
    - The CSIRT must build or purchase a robust tracking system.
    - Distributed staff members may be unwilling to take on the additional responsibility unless they perceive some value in the work or receive additional compensation for it.

8 Coordinating CSIRT

8.1 Overview

In this model the main focus of the CSIRT is to coordinate and facilitate incident and vulnerability handling activities across a broad, diverse, and usually external constituency. This coordination and facilitation can involve sharing information, providing mitigation strategies and recommendations for incident response and recovery, researching and analyzing trends and patterns of incident activity within the constituency, providing resources and references for incident management such as vulnerability databases, clearinghouses for security tools, or advisory and alert services.

There are different types of coordinating CSIRTs and each has a different level of authority in relationship to the supported constituency. One type of coordinating CSIRT may serve a specific constituency group—for example, a coordinating CSIRT for a multinational corporation. In this case the CSIRT may have authority to implement incident response solutions and mitigation strategies across the organization. However, it can be the case that the international pieces of the corporation are affiliate companies and not under the jurisdiction of the CSIRT.

Another type of coordinating CSIRT may serve a constituency made up of the various branches of a country's military. In this case, the CSIRT may have authority over all members of the constituency.

Another type of coordinating CSIRT may serve a whole country, province, or state. In this case the CSIRT will not necessarily have authority over the constituency. The same can be said for a CSIRT for a large or national research network, educational institution, or the general public. For example, the Internet community (which includes computer security experts as well as the general public) is the constituency for the CERT/CC. However, the CERT/CC has no authority over anyone within this constituency, but can affect change based on the value of the information and service provided to the constituency.

When the coordinating CSIRT has no authority, it can only act as an advisor to the constituency. It cannot make any decisions or take any actions on its own for specific systems that are affected. The coordinating CSIRT can provide high-level analysis and suggest recovery and mitigation strategies, but it is up to the constituency to decide to follow the recommendations.

The coordinating CSIRT may be able, because of its position and reputation in the constituency, to influence the decision-makers to act for the overall good of the organization.[47]

Whatever the type of coordinating CSIRT, it always serves a distributed constituency. Usually the constituency consists of multiple, independent entities, however, they may be in similar sectors such as various military or financial organizations. These entities may even have their own internal CSIRT. In such cases, the coordinating CSIRT interacts with the internal CSIRT as a point of contact. Information and recommendations are passed on to the internal CSIRT, whose members then choose what to pass on to their own constituency.

8.2 Supported Constituencies

As already mentioned in the overview, this model concentrates on the coordination of many independent entities. Usually such entities are organizations that share some common characteristics that make them part of the team's constituency. Common characteristics that are usually found today are

- network connectivity, e.g., national research networks such as the Computer Emergency Response Team for the German Research Network DFN (DFN-CERT)

- geographical boundaries, e.g., Japan Computer Emergency Response Coordination Center (JPCERT/CC)

- organizational boundaries, e.g., SIEMENS-CERT for the organizations in the SIEMENS group

- general public or support for other CSIRT organizations, e.g., CERT/CC and FIRST

Coordinating CSIRTs have a long tradition, starting in the early 1990s, of providing incident response services in multi-organizational constituencies (e.g., CERT/CC), and especially in the European research networks, the SURFnet Computer Security Incident Response Team (CERT-NL) and DFN-CERT are popular examples. While CERT-NL and DFN-CERT coordination efforts were focused on a particular bounded domain (a national research network), their informal constituency was much larger in practice. Being the only CSIRT available, at that time, in a specific country made them in reality the "default" coordinating CSIRT on a national scale. Although this posed some practical challenges to CERT-NL and DFN-CERT related to workload, charter, and authority, as time progressed and the development of other teams increased, the burden of being a default coordinating body for the unbounded constituency lessened. That being said, sometimes these CSIRTs still receive requests for assistance

---

[47] If the coordinating role is assigned within a group of organizations that have contractual or legal relationships, such as an industry group or holding company, stronger means of authority might be applied. For example, if the coordinating CSIRT reports to the board of the holding company, its advice might be presented to the organizations within the holding company in a way that has a great deal of authority, not defined by the coordinating CSIRT, but by the board.

from these broader constituencies, even though there are other, more applicable CSIRTs that should be contacted. AusCERT, for example, although a membership-based CSIRT, still is contacted by other external groups who are seeking help in notifying sites in Australia concerning incident activity.

Today there are a number of CSIRTs that coordinate larger multi-organizational constituencies[48] like the U.S. military, the U.S. federal government, various research networks, and to some degree the commercial entities that are peers within a single country. National CSIRTs, for example, will participate in coordination efforts across their constituency and probably with other national CSIRTs but concentrate their efforts locally at their constituency level in their day-to-day operations.

Some countries establish one coordinating CSIRT for a whole nation by providing government funding. An example of this would be SingCERT, which serves the Internet community in Singapore.

In countries where no other country-level coordinating CSIRT has been established, an existing CSIRT may extend its services to the bigger, informal constituency, making it in fact a national CSIRT. CERT-NASK, for example, became CERT-Polska early in 2001 and is now serving the Internet community in Poland.

Other coordinating CSIRTs may service a particular geographic region or sector. For example the Asia Pacific Computer Emergency Response Team (APCERT) works to coordinate CSIRT activity in the Asia Pacific area. The TERENA Task Force "CSIRT Coordination for Europe" (TF-CSIRT) does similar coordination work for the European Community.

8.3   Organizational Structure

As the coordinating CSIRT is most likely a dedicated team, it has a central location and manager.[49] Ideally, the CSIRT comprises staff with expertise in all systems and platforms supported by the constituency. However, if the constituency is made up of many single, independent organizations, this is not usually possible. In that case, experts from the constituency or other trusted computer security organizations need to be identified to work with the team as needed. The CSIRT staff contains positions for triage and hotline handling, incident analysis,

---

[48]   For example: U.S. military (DOD-CERT); U.S. Federal Government (FedCIRC), country-wide CSIRTs such as the Singapore Computer Emergency Response Team (SingCERT); or CSIRTs that have research/academic networks as their constituencies, such as CAIS – Brazilian Research Network CSIRT (CAIS/RNP).

[49]   Most often teams that fit this category are centralized. In some cases distributed teams or combinations of distributed and centralized teams can be found. For this document we describe the model most often observed.

support, response, and coordination. The coordinating CSIRT may also have staff that perform vulnerability and artifact handling services. Administrative support staff is also required.

Although it is up to the coordinating CSIRT to determine what services to offer, the constituency can often influence what is provided based on their needs. Since a coordinating team in a large, geographically dispersed constituency cannot reasonably provide direct incident response on site, and since the coordinating CSIRT should not compete with the constituency's internal CSIRTs, the services generally provided will complement existing local services or provide value-added services not provided within the constituency. The main functions of the coordinating CSIRT are to act efficiently as the coordination center and to direct the response effort at various levels of the organizations that make up the constituency by providing advisories, alerts, training sessions, documented policies and procedures, and expert guidance. The coordinating CSIRT, acting as a neutral party, is able to synthesize information to form a high-level view of activity and then provide detailed analysis to those constituent members who do not have available resources or expertise.[50] Many of these teams may need to rely on the coordinating CSIRT's analysis and guidance to determine appropriate response strategies.

8.4   Triage

In a coordinating CSIRT environment, the triage function is central to the operation of the team. It is a clearly defined point of contact. There are advertised descriptions of the services provided, hours of operation, and guidelines for how and what to report. Online reporting guidelines and online references are available to assist the constituency's staff in reporting and contacting the coordinating CSIRT.

Identified staff in the coordinating CSIRT perform the triage function. Explicit guidelines for what requests and reports are handled and what are not handled are developed and used by staff to assist in performing this service.

8.5   Available Services

The following sections describe services that might be provided in a coordinating CSIRT model. It is recognized that every team is different, so these are general descriptions based on observations of and discussions with other teams. The method in which the service is delivered assumes a certain level of infrastructure, staff, and equipment, which are discussed in further sections.

---

[50]   If the coordinating CSIRT is co-located with one of the organizations of the constituency, great care must be taken to not risk this neutrality.

8.5.1 Core Services

Because of the structure and operational goals of a coordinating CSIRT, the following services tend to be the basic ones most often provided, although they are somewhat different from the normal core services discussed in Section 2.7.4.[51]

Alerts and Warnings

Since the first CSIRT was created, this service has been part of the core set of services offered by coordinating CSIRTs. In the day-to-day operations, CSIRTs receive and triage all incoming information, especially concentrating on events that point to any risk the constituency might face. As part of the CSIRT work, they forward all information concerning alerts and warnings to the points of contact in their constituency. They also may create their own alerts and warnings based on information and research collected. Once information is distributed to identified points of contact, it is up to these points of contact to determine how much further this information is distributed within the constituency and to whom the information is disseminated.

After any distributed alert or warning, the coordinating CSIRT collects and evaluates feedback from the constituency to re-evaluate and further refine the assessment to better serve the constituency. As any feedback would be voluntary, this re-evaluation may be based on a low number of responses, rather than based on feedback from the whole constituency. The information could also be based on further research and analysis that the coordinating CSIRT performed itself.

Incident Analysis

The coordinating CSIRT undertakes analysis of incident reports received to determine the nature of the activity being reported, what intruder tool(s) were used, the scope of the activity, and the appropriate recovery or mitigation strategies to be applied. They are not usually reviewing incident artifacts and logs to recover a particular system, but to see what the basic attack strategy was, so they can correlate this information with other activity across the broader constituency. In-depth analysis or forensic analysis on affected systems would be done by the constituency's local CSIRT or security team.

Since a coordinating CSIRT most likely does not receive reports regarding every individual incident occurring in its constituency, it must make estimations of the scope and threat impact based on the reports it does receive.

The CSIRT performs incident analysis to understand what is occurring in the constituency. Based on its understanding of the overall picture, the CSIRT makes recommendations for strengthening overall security when possible. It is able to identify high-level intruder trends

---

[51]   Again, your experiences or requirements may differ.

and attack methods, and use this information to provide suggested strategies for securing and defending constituent systems.

Incident Response Support

Because the coordinating CSIRT is not on site and not devoted to one specific constituency, its main focus will be to provide support to many constituency organizations, which could include other CSIRTs. This support can take various forms depending on the needs of the overall constituency. Supporting activities can include

- answering questions via phone or email from constituents or their respective CSIRTs

- researching and analyzing incidents, vulnerabilities, and artifacts, and providing the resulting information to the overall constituency

- maintaining an archive of incident, vulnerability, and artifact information that is accessible by the constituency

- creating and disseminating advisories and alerts with recovery and response strategies

- creating technical documents outlining response steps and security best practices

- developing appropriate user awareness, education, and training materials for the constituency

Information can be disseminated via intranets or extranets, email, phone, or mailing lists. Each constituent entity determines who receives the information and assistance and who follows any distributed guidelines to perform the response operations and tasks.

Incident Response Coordination

In a coordinating CSIRT model, the incident response coordination service is one of the main services or functions of the team. With dedicated resources, the team can provide comprehensive tracking, recording, and dissemination of information for the constituency. By consolidating collected information, the team is better able to identify similar attacks, artifacts, exploits, trends, and patterns. Potential new threats to the constituency can also be identified and mitigation strategies developed and distributed. The coordination work done in this model is more a matter of information exchanging and facilitation of interactions between the parties involved in the recovery or analysis of the ongoing incident activity.

In this model, although it is desirable it is unlikely that the team will have expertise or familiarity with all platforms and operating systems inside the constituency. Therefore it will need to call upon external experts from constituency sites, vendor organizations, other computer security organizations or other CSIRTs to assist in the actual analysis. The coordinating CSIRT can act as a facilitator or a main point of contact for bringing these various organizations together. It can also be a main distribution point for disseminating the resulting response or mitigation strategies to the rest of the constituency.

Because the coordinating CSIRT is a well-known point of contact for its constituency, it may receive warnings and alerts from other organizations that need to be redistributed to the sites and constituents involved.

Vulnerability and Artifact Response Coordination

Similar to the way that the coordinating CSIRT provides incident response coordination, it can also be effective in providing vulnerability and artifact response coordination. These coordination functions are possible because of the wider variety of information the CSIRT is able to gather and analyze from its diverse constituencies and because the CSIRT has more time to devote to collecting and analyzing the information. This ability to collect and synthesize information that can be shared with the various components of the constituency is one of the greatest benefits of the coordinating CSIRT.

Another part of this coordination effort is to inform constituents about the results of various analyses of vulnerabilities and artifacts along with any remediation strategies.

Announcements

Because the CSIRT has access to information from the various organizations within its constituency and from other security experts and groups, it can present a broad picture of incident activity to the constituency. It can do this through general announcements based on this comprehensive information. These announcements are intended to raise the awareness of the constituency towards new trends and areas of concern for the security of the constituent organizations or of the constituency at large. The coordinating CSIRT also can provide information to help the constituency proactively defend its critical assets. This may take the form of letting constituents know of newly found vulnerabilities and artifacts, so they can check their systems and remove or fix the problems before they are exploited.

Technology Watch

This service is another that can be provided by the CSIRT to the constituency as a value-added service. The members of the coordinating CSIRT can focus more time on performing a technology watch function than most of their constituent organizations, due to their dedicated staff. This can be an extremely beneficial resource provided by the CSIRT.

Individuals on the coordinating CSIRT are assigned this function for the various supported technologies and platforms as resources are available. The information they collect is consolidated to highlight current attacks, threats, trends, and other relevant items. This synthesized information is made available to the rest of the CSIRT staff via a secured intranet or extranet and is then, in turn, used to further create value-added information for the constituency.

Security-related information that is of interest to the constituency can be posted to a mailing list or an Internet discussion site as a method of keeping network, system, and security admin-

istrators up to date. It can also be used to raise the level of security awareness for all members of the constituency. Such a site can provide educational benefits by allowing people to post questions that can be answered by the CSIRT staff if time permits.

Security-Related Information Dissemination

The coordinating CSIRT may be able to provide this type of service for its constituents who do not have time and resources to collect and disseminate this information.

To provide the constituency wide access to security-related information, the CSIRT can establish a centralized web site (and corresponding FTP site if necessary.). The coordinating CSIRT collects information on security trends, best practices, and tools, and provides this information to either its points of contact or to the whole constituency. If desired, recommended tools and software updates or patches can be made available to provide authenticated versions for reference in alerts and warnings.

As with the centralized CSIRT model, coordinating CSIRTs may provide translation services to distribute security information to the constituency in their native language.

Awareness Building and Education/Training

Most coordinating CSIRTs engage in some form of awareness building, education, or training for their constituency. This might involve developing training classes on security and incident response issues, tutorials on attack types and mediation strategies, or even research into incident and vulnerability trends. Because of this, we include these services in the core services list for coordinating CSIRTs.

Members of the coordinating CSIRT may be assigned to visit constituency site locations to provide briefings or security awareness training. CSIRT staff can also provide instruction on security issues, tools, and recovery techniques. Sometimes this is done as a for-fee service, and sometimes it is done as a free member service.

8.5.2 Additional Services

In addition to its core services, a coordinating CSIRT may choose to offer other services. The following services are those most likely to be provided.

Vulnerability and Artifact Analysis

A coordinating CSIRT may have the means, expertise, and time to analyze various vulnerabilities or artifacts that it receives through reports or through its own research, while its constituents may not have the time or the expertise to do this type of work. The CSIRT can focus on those vulnerabilities and artifacts that might have a potential impact on its constituency, or it

may analyze vulnerabilities and artifacts to provide general public information rather than information specific to the constituency.

.A good example of this can be seen in some of the work done by the CERT/CC. This coordinating CSIRT provides a knowledgebase of vulnerability information to the public. The CERT/CC has dedicated staff to analyze reported vulnerabilities and work with vendors to determine the status of a vulnerability in various products. This is not a service that many CSIRTs have the time or resources to perform. Many different constituencies can benefit from this work, without having to replicate this service at a local internal team level.

Vulnerability and Artifact Response

After completing the analysis of vulnerabilities or artifacts, any relevant information for mitigating or repairing a vulnerability or detecting and removing an artifact is passed on to the constituency. This information may be distributed as an alert, advisory, or even as a technical document. For example the CERT/CC provides vulnerability information and mitigation strategies via the Vulnerability Notes database and the Vulnerability Reports Catalog, both pieces of the CERT/CC Knowledgebase.[52] In a similar manner, MITRE's Common Vulnerabilities and Exposures (CVE) database also provides information about and a catalog of vulnerabilities.

Usually this response effort is limited to the provision of information and mitigation strategies. However, some CSIRTs may offer additional for-fee services that involve traveling to a site to help actually repair and recover affected systems. Others may provide a fee-based service to help sites install patches.

Development of Security Tools

With the proper staff time and expertise, members of a coordinating CSIRT may become involved in developing security tools that may be used by members of their constituency or by other CSIRTs. For example, the CERT/CC has developed tools such as AirCERT (Automated Incident Reporting) and specialized secure mailing tools. JANET-CERT and DFN-CERT are involved in developing various incident tracking systems. Other teams may develop virus or IDS signatures or other tools, scripts, and patches for use in response activities.

Other Services

Generally a coordinating CSIRT does not provide services involving configuration and maintenance of security tools, applications, and infrastructures; security audits or assessments; or intrusion detection. However, in rare instances, these can be provided as for-fee services, if the team has the time and expertise to perform these functions.

---

[52] For more information see <http://www.cert.org/kb/>.

8.5.3 Impact on Security Quality Management

In most cases the coordinating CSIRT does not work with other parts of the constituency to provide security quality management services. Instead it provides general guidelines that can be used by members of the constituency to improve the overall security of their enterprises. An exception to this is if the coordinating CSIRT was hired in a consulting or managed security service provider capacity to specifically perform these services. Another exception to this would be if the coordinating CSIRT was actually coordinating other internal CSIRTs within the same organization, such as a coordinating CSIRT in an educational institution that coordinates activity across other CSIRTs at branch campuses.

Services that the coordinating CSIRT might be hired to perform if they are external to the constituency or that the CSIRT might coordinate if they are an internal coordination center include providing security consulting and assisting with the development of security policies and business continuity plans.

Other services that the coordinating CSIRT might provide include the development and delivery of training courses, tutorials, and security awareness briefings. These have been included previously under "Core Services," as most coordination CSIRTs provide these services.

8.6 Resources

The following staffing, equipment, and infrastructure resources should be considered when implementing a combined CSIRT model.

8.6.1 Staff

A coordinating CSIRT provides a core staff that devotes 100% of their time to coordinating the incident handling activities of their constituents.

This staff contains the following individuals:

- one manager (and designated backup)
- one administrative support person
- several (typically 3 to 10) technical staff. Staff size will depend on the size of the constituency and the services offered. Staff may do not only technical analysis and incident handling work but also provide training and instruction.
- one or more system administrators to provide infrastructure support
- one or more hotline/triage/help desk staff

The size of the team will be determined by the size and diversity of the constituency. For additional tasks and functions that support the work of the core staff, arrangements need to be made in advance with

- technical writers
- public affairs staff
- legal/criminal investigators

The coordinating CSIRT can also cooperate and collaborate with other security or organizational experts from within the constituency when specialized expertise is required.

8.6.2 Equipment

Equipment is needed to support the coordinating CSIRT staff, similar to the requirements for the internal centralized CSIRT. This includes (but is not limited to) the following:

- office space and furniture (desks, copier, supplies, etc.)
- computer equipment for day-to-day operations and activities
- non-production test lab facilities
- travel and home equipment (for remote access, training, and on-site visits)
- telephones (secure telephones, fax, cellular, pagers)
- other ancillary equipment for testing as necessary to support provided services

8.6.3 Infrastructure

The infrastructure provides a secure environment for CSIRT day-to-day operations. This includes (but is not limited to) the following:

- physical security
- protected power sources and generator (if appropriate)
- a firewall or separate network to isolate the CSIRT network from any other network
- network and host security
- secure intranet
- a robust and secure tracking system (trouble ticket system, relational database, etc.)
- secure repository for storing and archiving all incident and vulnerability related data and reports
- secure communications support (email, phone, faxes, videoconference, etc.)
- web services

- encryption technologies

- virus protection and scanning software

- secure backups and storage of CSIRT data

If the coordinating CSIRT is hosted by another organization, it can take advantage of some of its network infrastructure. Great care must be taken to ensure the confidentiality of incident and vulnerability data, therefore a firewall to isolate the CSIRT local network is highly recommended.

One of the most important infrastructure components needed for a coordinating CSIRT to interact with its constituency are formal, secure methods for collecting and disseminating computer security information, incident reports, vulnerability reports, and other alerts or warnings.

8.7 Summary

This model is fundamentally different from the other models described in this handbook, although many of the components and services may be similar to those previously discussed. Since a coordinating CSIRT is established to serve the interests of a larger constituency that potentially comprises hundreds of independent entities rather than a single organization,[53] the manner in which services are delivered can be very different from the way they are provided by internal CSIRTs.

8.7.1 Impact on Constituency

Since the coordinating CSIRT is not usually involved in the actual recovery of systems or in securing compromised internal systems for the constituency, it can concentrate on coordinating activities between multiple independent parties and provide a level of neutrality not otherwise achievable. It maximizes the utilization of a relatively low number of staff in one strategic location and provides the central coordinating capabilities to allow a broad understanding of the security threats and activity affecting the constituency. It can quickly synthesize information available from a wide variety of constituent sources and disseminate it to the organizations in the constituency.

This team responds to reports of abnormal activity and incident reports, participates in incident and vulnerability analyses, and plays a proactive role in promulgating computer security awareness throughout the constituency. It also acts as point of contact for other CSIRTs that want to report incidents involving sites in the constituency. Coordinating CSIRT members col-

---

[53] The coordinating CSIRT might be hosted in one entity that is also part of the constituency, but from a service provider point of view, the hosting organization is no different from any other entity in the constituency. There are differences in some cases; for example, attacks (such as DDoS attacks) on the hosting organization will affect the coordinating CSIRT as well, and vice versa.

laborate and participate in security-related working groups or workshops, promote security awareness and training, and lend their expertise in testing and analysis activities.

The main impact on the constituency is to understand what type of interaction they can expect with the coordinating CSIRT, how and when to report information, and how to receive and follow any guidelines or recommendations coming from the coordinating team.

To be successful in its coordination role, the CSIRT must be trusted by the constituency, provide value-added services to the constituency, and have established points of contact and communication mechanisms for interacting with the constituency. These should include special secure communications technologies, use of encryption or authentication technologies, and specialized mail distribution lists. Having a complete and verified list of points of contact within the constituency will help determine who should be notified when information is distributed and will reduce the time needed to disseminate the information appropriately.

8.7.2 Constraints

The main constraints in this model are the difficulty of building effective relationships with all entities in the constituency and gaining their trust so that incidents are reported and recommended mitigation and prevention strategies are followed. Operating across a large geographical area with multiple time zones adds to the difficulties a coordinating CSIRT may face. If coordination takes place in an even broader context, differences in language, culture, and laws can create difficulties in providing an appropriate level of assistance to all involved parties.

Other constraints include ensuring that the coordinating CSIRT works together effectively with the organizations in its constituency. This is especially true as coordinating CSIRTs almost always have no authority over their constituency and serve in an advisory capacity, making it difficult to enforce any recommendations or guidelines, even when there are widespread attacks.

Because the coordinating CSIRT may not have direct authority, members of the constituency can choose to ignore its advice and recommendations. They can also choose to handle incidents on their own without reporting activity to the coordinating CSIRT. This can limit the amount of information the coordinating CSIRT has to work with in determining the scope, nature, and impact of any activity or threat.

Another constraint can involve the parent or hosting organization for the coordinating CSIRT. If this host organization does not have a trusted reputation in the constituency, this can affect how the CSIRT is perceived and cause constituents to fail to report to the coordinating CSIRT. Very often a coordinating CSIRT survives on its reputation, along with the accuracy and value of its services.

Finally, a problem may result regarding the expectations that the constituent members have versus the actual services offered by a coordinating CSIRT. The constituent may want a deeper level of service provided than the CSIRT is able to provide. For example, the constituent may want someone to come to their site to help in the recovery and response efforts, and this may not be a provided service.

8.7.3 Strengths and Weaknesses of the Model

The main strength of this model is that it provides a stable core of CSIRT professionals, in one central place, who are tasked with coordination. The full-time members provide stability, expertise, and a permanent infrastructure.

The greatest weakness to this approach is that the team might lack the operational knowledge and the ability to address the operational units in its constituency. If this issue is not handled well, it can result in a team that is not accepted and therefore does not receive incident reports and has little impact on the constituency.[54]

The strengths and weaknesses of this coordinating model include the following:

- Strengths
  - There is a dedicated staff trained in computer security response and coordination.
  - There is a focused, dedicated responsibility for performing incident response coordination.
  - There is a central point for incident reporting, analysis, and response across the organizations in the constituency.
  - There is a central point for analyzing information to determine trends and patterns for the entire constituency.
  - There is a central repository for incident, vulnerability, and artifact data from the entire constituency.
  - There is a focal point for incident reporting from outside the constituency where the coordinating CSIRT accepts incoming reports and forwards them, with supporting information, to the organizations involved.
  - The CSIRT can use the obtained information and analysis to provide valuable information to the constituency (advisories, alerts, warnings, technical documents, checklists, best practices, etc.).
- Weaknesses
  - It is difficult to coordinate with all entities in large and disperse constituencies.
  - The coordinating team may seem isolated from the rest of the organizations in the constituency.
  - The constituency may need to fund the coordinating CSIRT.

---

[54] Depending on the environment and other circumstances, support by experts from the constituency might be made available or arranged. This can reduce this particular weakness.

- It is difficult to determine the correct size of the staff.
- It can be difficult to get buy-in from organizations to follow CSIRT recommendations.
- It is difficult to manage and coordinate coverage in all the areas of expertise necessary at an in-depth level.
- Finding experts in the constituency may be cumbersome, and over time there can be problems with turnover, as well as training issues.
- It is difficult to ensure that all entities within the constituency respond to incident reports and act on recommendations in a timely, appropriate manner.
- It is difficult to ensure that security alerts and announcements are distributed to the right units in constituent organizations.
- Information may have to flow through several organizational layers (coordinating CSIRT, internal CSIRT, and security team), causing delays in response and recovery time.
- The coordinating CSIRT needs to build or purchase a robust tracking system.
- It can be difficult to explain how the coordinating CSIRT provides value-added service to participating organizations and thereby gain their willingness to accept reporting incidents to the CSIRT and accept recommendations from the CSIRT.
- It is difficult to keep the points of contact for each participating constituent member up to date.
- The organization that is the parent or host organization for a CSIRT can impact the way the CSIRT is viewed in the community. If the host organization is not trusted or respected this may have an adverse effect on the CSIRT and its staff.

9 Choosing the Right CSIRT Model for Your Organization

In the preceding sections, we have outlined a number of different models and CSIRT services to help you understand the options available. Of course, you can pick the most applicable features from each of the models described and design your own CSIRT model. Or perhaps your organization will require multiple organizational models to fit the needs of your situation. If you are still not sure what type of model would work best for your organizational structure, the guidelines in this chapter for choosing a model might help.

Please be advised that any answer that might be determined from the information below should be seen as a guide rather than a definitive recommendation. A definitive recommendation would require much more specific information about your constituency, mission, and services.

9.1 Do We Describe Your Team in this Handbook?

Although we have described several organizational models for implementing a CSIRT capability, this handbook is not inclusive. Specifically, we do not provide a model of operation for a vendor team or a managed security services provider. There may also be various situations that require a custom model for organizations.

If your team concentrates on security vulnerabilities as part of a vendor company, that is, your team receives reports of security flaws in your vendor products and works to repair these flaws and provide alerts, advisories, and fixes related to these flaws, then you are considered a vendor team. Since we do not provide a model for vendor teams, you may be able to discern a model yourself, based on the advantages and disadvantages described for each model in this handbook.

If your team provides incident response or security services to customers for a fee, then you are most likely a managed security services provider. We also do not provide a model for this type of team. Some of the models presented here may work for your organizational structure, but you will need to review the advantages and disadvantages of each and see which best suits your situation.

9.2 Are You a Security Team?

If you meet the following criteria, then you are probably a security team and should read Chapter 4.

- There is no designated group responsible for incident handling.

- Members of existing infrastructure, IT, and security groups handle any computer security incidents and problems, as part of their normal day-to-day work.

- Members of the security team perform on-site incident response.

9.3 Are You a Coordinating CSIRT?

If you meet the following criteria, then you are probably a coordinating CSIRT and should read Chapter 8.

- Your team does not belong to the same organization as your constituency.

- Your team coordinates incident response efforts and information exchanges across many different CSIRTs, security teams, and/or other external organizations.

- Your main services are to coordinate information exchanges and facilitate discussions of incident activity. You do not perform on-site incident response.

9.4 Are You an Internal CSIRT?

If you meet the following criteria, then you are probably an internal CSIRT.

- Your CSIRT is in the same organization as your constituency.

- The main priority of your team is to focus on incident handling rather than being responsible for maintaining any other part of the security infrastructure.

- Specific authority and responsibility for handling incidents has been given to your team.

There are three different models for internal CSIRTs: distributed, centralized, and combined. Read the following information to determine what type of model may work best for you.

While it is rather straightforward to differentiate between the main categories of organizational models—security team vs. internal CSIRT vs. coordinating CSIRT, deciding whether a centralized approach would be better than a distributed or combined one for an internal CSIRT may be difficult. Instead we will discuss some of the factors that influence any decision.

- **Size and Distribution of Constituency**

  This refers to how big the constituency is (the part of the organization your team is responsible for). Size can be measured in terms of users as well as number of networks, internet connections, and systems to protect.

  A small or mid-sized organization may only need a small centralized team, while a large organization usually implies that staff are spread out among more departments, buildings, or even geographic locations and may require a more distributed team to adequately accommodate the variety of systems, locations, and staff. Much more difficult to handle than geographic locations are time zones and language differences. Both make it difficult to serve constituent members efficiently.

- **Services Provided and Related Service Levels**

  If for example your team provides incident response on site instead of incident response support, this implies that you can be on site in a reasonable time period (otherwise it would not make any sense to provide that service). Depending on the service and related service levels negotiated, this is best provided by a distributed model or combined model, where part of the CSIRT capability is located at distributed sites.

  The type of mission and function of the CSIRT as expressed by the services provided has a great impact on the type of organizational model that will be needed. The provision of certain types of services may require a particular organizational model to be effective. If the CSIRT's main function is to perform analysis and repair and recovery tasks, then in many cases a distributed or combined model would work best, especially if there should be close cooperation between the CSIRT and other staff or teams. On the other hand, if the purpose of the CSIRT is to collect information across the organization, provide support in cases of incidents, and propose recommendations and solutions, then a centralized CSIRT may work best.

- **Funding and Resources**

  This refers to the amount of funding or the budget available for creating and operating the CSIRT. If there is limited funding available, the organization may have to rely on a security team with an established incident response process rather than a formalized CSIRT. Another option might be to form a distributed team by using existing staff and only adding a new CSIRT manager position. A third option might be a small centralized team. If sufficient funding is available, larger and more complex models based on more staff may be an option. Even low funding levels can allow for a small, effective centralized CSIRT, if the services provided and the service levels are in line with the amount of funding and resources available.

- **Position in the Organization**

  While this factor cannot be influenced in most cases, it has a strong impact. In fact, for the internal setup of a CSIRT, the department that drives the development will greatly influence the organizational model chosen. Experience shows that a CSIRT usually starts out as an activity of the IT department, in which case technical issues and services are the

main focus. A CSIRT may also evolve from the security/risk management or policy department, in which case the team will be much more focused on policies. Depending on the organizational structure that the responsible department has, the CSIRT will follow the intent and purpose of its originating entity. Only if the CSIRT will be established outside the existing "founder" will its model possibly change.

Related to this observation, in organizations with existing security teams, it might be possible to enhance those teams. Depending on the approach chosen, the organizational model for the CSIRT will become more centralized if one of the security teams is selected as the foundation of the CSIRT. The organizational model will become distributed if responsibilities for incident handling are given to all security teams already distributed across the organization.

The following are a few examples of choosing an organizational model based on combinations of various factors.

- A small educational institution with little or no funding will continue to depend on their security teams, which require no additional funding. However, it is recognized that these types of teams do not provide good coordination or analysis of incidents beyond responding to them to recover and repair systems.

- The same small educational institution would benefit from a small centralized CSIRT, which, although requiring some additional funding, could provide a centralized location for incident reporting, analysis, and response.

- If the institution is too small and has no effective security teams already in place, then instead of concentrating on developing a CSIRT, emphasis may be placed on developing a security team with more staff and added responsibilities for incident handling.

- For a large, multinational financial corporation with multiple affiliates and subsidiaries, a combined CSIRT with a centralized staff devoted to monitoring incidents across the organization and recommending security precautions and solutions might provide a suitable approach. The team members are chosen from each affiliate, subsidiary, and remote site as members of the distributed part of the combined CSIRT.

- If in the large, multinational financial corporation the CSIRT has no authority over the affiliates and subsidiaries, a coordinating CSIRT within the headquarters will provide a much more effective structure. The coordinating CSIRT will work with CSIRTs at the affiliate/subsidiary level.

- If in the large, multinational financial corporation the CSIRT has no authority over the affiliates and subsidiaries, the CSIRT might still be responsible for IT components such as the centralized backbones, Internet connection points, and critical infrastructure elements within the authority of the corporate headquarters. In such cases the CSIRT should be monitoring these elements and should handle—with authority as appropriate—all incidents that they become aware of. The centralized nature of these functions may make a centralized CSIRT feasible, or again a combined CSIRT might also work.

10 Closing Remarks

The focus of this document has been the presentation of several organizational models for providing a CSIRT capability. While there is no "best" model, each one of them has distinct benefits for a particular situation or environment. Care has been taken to elaborate on the description of possible services to help you make an appropriate selection of a model in terms of a package of services. It is important to note that there is no easy answer for which model would best suit an organization; each organization's structure and requirements must be carefully considered. Also, while not every organization will fit a specific model for a CSIRT, every organization needs to be prepared to address computer security incidents and problems in its day-to-day operations.

We have also described some of the issues an organization is likely to encounter in the delivery of incident handling services. It is our hope that the descriptions for how delivery of each service might work within the models has helped you gain a better understanding of the strengths and limitations of each model.

Once your organization has selected a model, you should refer to the *Handbook for CSIRTs* [West-Brown 03] to learn more about how to implement and operate your CSIRT.

If you have comments about any of these models or if you know of a model that differs from those described here (or offers other services we haven't described), let us know. Please email us at csirt-info@cert.org with any comments, criticisms, or recommendations concerning this document, *Organizational Models for CSIRTs*. We'd like to hear from you.

Appendix   Summary of Services Offered

The chart on the next two pages summarizes the services offered by each type of CSIRT described in this handbook. The services are categorized by type and according to the following:

Core: A basic service provided by the members of the team

Additional: A service that can be provided if the appropriate resources and expertise are available

Unusual: A service not generally provided by this type of team, unless special circumstances exist

Service Category	Services		Security Team	Distributed	Centralized	Combined	Coordinating
Reactive	Alerts and Warnings		Additional	Core	Core	Core	Core
	Incident Handling	Incident Analysis	Core	Core	Core	Core	Core
		Incident Response On Site	Core	Additional	Additional	Additional	Unusual
		Incident Response Support	Unusual	Core	Core	Core	Core
		Incident Response Coordination	Core	Core	Core	Core	Core
	Vulnerability Handling	Vulnerability Analysis	Additional	Additional	Additional	Additional	Additional
		Vulnerability Response	Core	Additional	Unusual	Additional	Additional
		Vulnerability Response Coordination	Additional	Core	Core	Core	Core
	Artifact Handling	Artifact Analysis	Additional	Additional	Additional	Additional	Additional
		Artifact Response	Core	Additional	Unusual	Additional	Additional
		Artifact Response Coordination	Additional	Additional	Core	Core	Core

Service Category	Services	Security Team	Distributed	Centralized	Combined	Coordinating
Proactive	Announcements	Unusual	Core	Core	Core	Core
	Technology Watch	Unusual	Additional	Core	Core	Core
	Security Audits and Assessments	Unusual	Additional	Additional	Additional	Unusual
	Configuration and Maintenance of Security Tools, Applications, and Infrastructures	Core	Additional	Additional	Additional	Unusual
	Development of Security Tools	Additional	Additional	Additional	Additional	Additional
	Intrusion Detection Services	Core	Additional	Additional	Additional	Unusual
	Security-Related Information Dissemination	Unusual	Additional	Core	Core	Core
Security Quality Management	Risk Analysis	Unusual	Additional	Additional	Additional	Additional
	Business Continuity and Disaster Recovery Planning	Unusual	Additional	Additional	Additional	Additional
	Security Consulting	Unusual	Additional	Additional	Additional	Additional
	Awareness Building	Unusual	Additional	Additional	Additional	Core
	Education/Training	Unusual	Additional	Additional	Additional	Core
	Product Evaluation or Certification	Unusual	Additional	Additional	Additional	Additional

Bibliography

URLs are valid as of the publication date of this document.

[Killcrece 02]   Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *CSIRT Services List*. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2002. <http://www.cert.org/csirts/services.html>.

[Killcrece 03]   Killcrece, Georgia; Kossakowski, Klaus-Peter; Ruefle, Robin; & Zajicek, Mark. *State of the Practice of Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-TR-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu/publications/documents /03.reports/03tr001.html>.

[Kossakowski 01]   Kossakowski, Klaus-Peter. *Information Technology Incident Response Capabilities*. Hamburg: Books on Demand, 2001 (ISBN: 3-8311-0059-4).

[West-Brown 98]   West-Brown, Moira J.; Stikvoort, Don; & Kossakowski, Klaus-Peter. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-98-HB-001). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 1998.

[West-Brown 03]   West-Brown, Moira J.; Stikvoort, Don; Kossakowski, Klaus-Peter; Killcrece, Georgia; Ruefle, Robin; & Zajicek, Mark. *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2003. <http://www.sei.cmu.edu /publications/documents/03.reports/03hb002.html>.

REPORT DOCUMENTATION PAGE

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. AGENCY USE ONLY (Leave Blank)	2. REPORT DATE December 2003	3. REPORT TYPE AND DATES COVERED Final
4. TITLE AND SUBTITLE Organizational Models for Computer Security Incident Response Teams (CSIRTs)		5. FUNDING NUMBERS F19628-00-C-0003
6. AUTHOR(S) Georgia Killcrece, Klaus-Peter Kossakowski, Robin Ruefle, Mark Zajicek		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213		8. PERFORMING ORGANIZATION REPORT NUMBER CMU/SEI-2003-HB-001
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) HQ ESC/XPK 5 Eglin Street Hanscom AFB, MA 01731-2116		10. SPONSORING/MONITORING AGENCY REPORT NUMBER
11. SUPPLEMENTARY NOTES		
12A DISTRIBUTION/AVAILABILITY STATEMENT Unclassified/Unlimited, DTIC, NTIS		12B DISTRIBUTION CODE

13. ABSTRACT (MAXIMUM 200 WORDS)

When a computer security attack on an organization occurs, an intrusion is recognized, or some other kind of computer security incident occurs, it is critical for the organization to have a fast and effective means of responding. One method of addressing this need is to establish a formal incident response capability or a Computer Security Incident Response Team (CSIRT). When an incident occurs, the goal of the CSIRT is to control and minimize any damage, preserve evidence, provide quick and efficient recovery, prevent similar future events, and gain insight into threats against the organization.

This handbook describes different models for implementing incident handling capabilities, including their advantages and disadvantages, as well as the kinds of incident management services that best fit with each organizational model. An earlier SEI publication, the *Handbook for Computer Security Incident Response Teams (CSIRTs)* (CMU/SEI-2003-HB-002), provided the baselines for establishing incident response capabilities. This new handbook builds on that coverage by enabling organizations to compare and evaluate CSIRT models. Based on this review they can then identify a model for implementation that addresses their needs and requirements.

14. SUBJECT TERMS CSIRT, computer security incident response team, incident handling, incident response, computer emergency response team, incident management, incident response management, CERT/CC, CERT Coordination Center, CSIRT models		15. NUMBER OF PAGES 156
16. PRICE CODE		

17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18 298-102